Bird & Bird

General Data Protection Regulation (GDPR) *Guide*

Contents

The General Data Protection Regulation *("GDPR")* is the European Union's cornerstone data protection law. It applies to almost all organisations doing business in or with the EU, or individuals in the EU. The *"Brussels effect"* means that many jurisdictions outside the European Union *("EU")* have followed GDPR concepts. So understanding the GDPR is important for businesses around the world.

This guide summarises key aspects of the GDPR and highlights the most important actions which organisations should take in seeking to comply with it.

We have divided our summary into sections which broadly follow those used by the GDPR, sub-divided into themes. Each sub-section starts with a speed-read summary and a list of suggested priority action points. We have also included a blue tab in each sub-section to guide you to where you can find relevant source material within the GDPR. We have also included details of key guidance materials published by European regulators who form the European Data Protection Board *("EDPB")* (and its predecessor the Article 29 Working Party).

We finalised the updates to this guide in December 2023 – by which date, we had seen a significant number of cases from the Court of Justice of the European Union *("CJEU")* analysing the GDPR. We have referenced these cases throughout the guide.

The European Union is also pursuing an ambitious digital agenda with multiple pieces of new legislation, which now complement the GDPR. We have indicated how the Digital Markets Act, Digital Services Act, Data Act, Data Governance Act and the NIS2 Directive need to be read alongside the GDPR. Although there is now also political agreement on the AI Act, as at the date of writing this introduction, there is no agreed text, so we have not (yet) included pointers to overlap with the AI Act. We will continue to update this guide to take account of new cases, guidance and legislation. If you would like to receive updates from us, please let us know. In the meantime, we hope that you will find this guide useful.

Material and territorial scope

At a glance

- The GDPR has extended the reach of EU data protection law:
  - An EU-based data controller or processor falls into its scope where personal data is processed *"in the context of the activities"* of its *"establishment"*. *"In the context of"* is a broadly-interpreted test, and the bar for what constitutes an *"establishment"* is low.
  - Where no EU presence exists, the GDPR will still apply whenever: (1) personal data relating to a data subject located in the EU is processed in connection with goods/ services offered to him/her; or (2) the behaviour of individuals located in the EU is *"monitored"*.
- Despite being a Regulation, the GDPR allows Member States to legislate in many areas. This has challenged the GDPR's aim of consistency, in areas such as employee data processing.
- The GDPR does not apply to certain activities – including processing covered by the Law Enforcement Directive[1], which was adopted as EU 2016/680 on 27 April 2016, for national security purposes and processing carried out by individuals purely for personal/ household activities.
- The GDPR has been in effect since 25 May 2018.

To do list

- ☑ Organisations (i) with an EU establishment or (ii) without an EU establishment but who monitor or target with goods/services EU-located individuals should:
  - understand the impact of the GDPR, and relevant case law/guidance which has clarified the application of its extra-territorial scope; and
  - determine an approach to compliance, and keep their compliance programmes under review.
- ☑ Organisations working in areas where "*special*"/sectoral rules are common should assess if they are required to comply with specific additional Member State laws and establish/maintain appropriate compliance programmes accordingly.
- ☑ Organisations should be aware that their processing may additionally be regulated (or soon be regulated) by the new *"Big 5"* EU data laws (the Digital Services Act, the Digital Markets Act, the Data Governance Act, the Data Act and the AI Act). The Big 5 may apply to personal data, but also to *"data"* more broadly (including non-personal data). Organisations will need to expand their digital regulation compliance programmes to cover these additional obligations.

1. Full title: EU Directive 2016/680 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, adopted on 27 April 2016

Territorial scope

EU "established" controllers or processors

Pursuant to Article 3(1), the GDPR applies to organisations which have EU *"establishments"*, where personal data is processed *"in the context of the activities"* of such an establishment. If this test is met, the GDPR applies irrespective of whether the actual data processing takes place in the EU or not.

"Establishment" was considered by the CJEU in the 2015 case of *Weltimmo v NAIH* (C-230/14). This confirmed that establishment is a *"broad"* and *"flexible"* phrase that should not depend on legal form. An organisation may be *"established"* where it exercises *"any real and effective activity – even a minimal one"* – through *"stable arrangements"* in the EU. The presence of a single representative may be sufficient. In that case, Weltimmo was considered to be established in Hungary notwithstanding that it was incorporated in Slovakia.

The EDPB guidelines align on territorial scope with the above case law, finding that *"the threshold for 'stable arrangement' can be quite low when the centre of activities of a controller concerns the provision of services online".* In some cases if, *"the presence of a single employee or agent acts with a sufficient degree of stability,"* that will suffice. However the EDPB does clarify that the mere presence of an employee in the EU may not be sufficient; the processing must also be carried out in the context of the activities of this employee – so the fact that an organisation has EU staff will not result in unconnected personal data processing becoming subject to the GDPR.

Organisations which have EU sales offices, which promote or sell advertising or marketing targeting EU residents will likely be subject to the GDPR - since the associated processing of personal data is considered to be "inextricably linked" to and thus carried out "in the context of the activities of" those EU establishments (CJEU case *Google Spain SL, Google Inc. v AEPD, Mario Costeja Gonzalez* (C-131/12)). The EDPB guidelines offer the example of a Chinese e-commerce website with an office in Berlin running commercial marketing campaigns towards EU markets. Because the Berlin office helps make the e-commerce activity profitable in the EU, the EDPB states that this would be sufficient to consider the Chinese company to be processing personal data in the context of its German establishment.

By contrast, the EDPB guidelines clarify that the accessibility of a website alone is not an establishment in the EU. This also mirrors CJEU case law – *VKI v Amazon* – which previously found that a website is not an establishment. The EDPB provides the example of a hotel chain that targets EU consumers but has no presence in the EU. The correct analysis would be under Article 3(2) (the extraterritorial provisions), not Article 3(1). The EDPB guidelines also confirm that just because an organization may be considered *"established"* for one activity will not render all its activities subject to GDPR.

Non-EU "established" organisations who target or monitor EU data subjects

Pursuant to Article 3(2), non-EU established organisations will be subject to the GDPR where they process personal data about EU data subjects in connection with:

- the *"offering of goods or services"* (payment is not required); or
- *"monitoring"* their behaviour within the EU.

For offering of goods and services (but not monitoring), mere accessibility of a site from within the EU is not sufficient. It must be apparent that the organisation *"envisages"* that activities will be directed to EU data subjects. In other words, the relevant determining issue will be evidence of intent. As listed in the EDPB guidelines, relevant factors include:

- references to the EU or a Member State in promotional material;
- paying a search engine to facilitate access to a website in the EU or launching a marketing campaign directed at an EU audience;
- the international nature of the activity, such as tourism-related activities;
- providing local phone numbers or addresses in association with a product or service;
- using top-level domain names that refer to the EU or a Member State (e.g. ".eu" or ".de");
- providing travel instructions from a Member State;

- mentioning international clientele or providing customer testimonials in promotional material, in particular where the customers are based in the EU;
- using an EU language or currency; and
- offering delivery services in the EU.

The EDPB guidelines do not state that any or all of these factors must be present for GDPR to apply, but rather that these are the sorts of indicators which supervisory authorities will look at when deciding if there is a sufficient intention to target individuals in the EU. It is not clear whether non-EU organisations offering goods and services to EU businesses (as opposed to individuals) will fall within the scope of the *"offering goods and services"* test in Article 3(2)(a).

"Monitoring": In contrast to offering goods and services, monitoring does not specifically require any indication of intent. Nonetheless, the EDPB guidelines state that *"the use of the word 'monitoring' implies that the controller has a specific purpose in mind for the collection and subsequent reuse of the relevant data about an individual's behaviour within the EU"*. The *"key consideration"* for identifying monitoring is the presence of *"any subsequent behavioural analysis or profiling techniques".* Profiling, as defined by GDPR, requires automated processing and the evaluation of *"personal aspects relating to a natural person"*, such as predicting health, personal preferences, economic situation, work performance or location or movements.

In other words, the passive collection over time of personal data concerning an individual's behaviour in the EU is not enough to constitute monitoring – there must be an evaluative purpose. The EDPB guidance provides a list of examples:

- behavioural advertising and geolocalisation of content (particularly for advertising);
- online tracking through cookies and device fingerprinting;
- an online personalised diet and health analytics service;
- CCTV;
- market surveys and other behavioural studies based on individual profiles; and
- monitoring or regular reporting on an individual's health status.

While the EDPB guidelines state that monitoring need not happen online (for example wearable technologies and other smart devices are clearly called out by the EDPB), it is interesting that most of the examples they provide are examples of online tracking. Other common use cases, such as anti-money laundering checks, email monitoring in the employment context and fraud prevention are not referenced.

The concept of *"monitoring"* is currently being considered in regulatory decision-making around Clearview AI, which compiled a database of facial data scraped from the internet. Several European regulators have argued that the GDPR applies to Clearview because the making available of its database *"relates to"* the monitoring by its customers of the individuals concerned.

In respect of all three Article 3 GDPR criteria (establishment, targeting and monitoring), a ruling on *Soriano v Forensic News* ([2021] EWCA Civ 1952) in the UK Court of Appeal suggests that the criteria may be interpreted more broadly than previously thought. The Court held that a group of US journalists associated with the Forensic News website had a *"reasonable prospect"* of fulfilling any of the Article 3 criteria (which means that the case is able to be heard). The Court said a *"minimal activity"* of publication subscriptions in the EU could constitute an establishment; that journalistic output could constitute *"offering"* services; and that the collection and sorting of journalistic data about an EU individual could constitute *"monitoring"*. However, following Brexit the case may have more limited impact in the EU as opposed to the UK, and has not yet been heard in full by the UK Court of Appeal.

Organisations subject to Article 3(2) of the GDPR must appoint an EU-based representative in one of the Member States where the data subjects whose data is processed are located. An equivalent obligation to appoint a UK-based representative currently exists under the UK GDPR too. The EDPB guidelines confirm that the GDPR does not establish substitutive liability for representatives: they can only be held liable for their direct obligations under the GDPR (i.e. Article 30 and Article 58(1)). Bird & Bird now assists non-EU and non-UK established organisations with this obligation and can be appointed as both UK and EU GDPR representative. Contact Bird & Bird Privacy Solutions if you would like further details about our GDPR representative services.

Where EU member state law applies by virtue of public international law

Recital 25 gives the example of a diplomatic mission or consular position. The EDPB guidelines also have the example of a cruise ship flying a German flag (because of its incorporation) in international waters. In this example, the cruise ship will be subject to the GDPR, according to the EDPB guidelines. A similar parallel could be made here with aircraft.

Exclusions

Certain activities fall entirely outside the GDPR's scope (listed below).

In addition, the GDPR acknowledges that data protection rights are not absolute and must be balanced (proportionately) with other rights – including the *"freedom to conduct a business"*. (For the ability of Member States to introduce exemptions, see section on derogations and special conditions). As the GDPR creates a strict regime in many areas of data protection, with arguably more sticks than regulatory carrots, businesses may find it helpful to refer back to this statement in Recital 4 as the need arises.

The GDPR does not apply to the processing of personal data (these general exemptions are very similar in the following cases to the equivalent provisions included in the Data Protection Directive):

- in respect of activities which fall outside the scope of EU law (e.g. activities concerning national security);
- in relation to the EU's common foreign and security policy;
- by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences and associated matters (i.e. where the Law Enforcement Directive applies);
- by EU institutions, where a specific instrument, Regulation (EU) 2018/1725, which came into force on 11 December 2018, aims to bring the rules for EU institutions in line with those set out in the GDPR. The rules are not however identical;
- by a natural person or as part of a *"purely personal or household activity"*. This covers correspondence and the holding of address books - but it also covers the social networking and online activities undertaken for social and domestic purposes. It represents a widening of the exemption from the principles set out in *Bodil Lindqvist* (C-101/01), before the advent of social media. In this case, the CJEU noted that sharing data with the Internet at large *"so that those data are made accessible to an indefinite number of people"* could not fall within this exemption, which it stated should be limited to activities *"carried out in the course of the private or family life of individuals"*. Note also that the GDPR remains applicable to controllers and processors who *"provide the means for processing"* which falls within this exemption.

The GDPR is stated to be *"without prejudice"* to the rules in the E-commerce Directive (2000/31/EC), in particular to those concerning the liability of *"intermediary service providers"*. These liability exemptions have now been replaced by equivalent (and updated) liability exemptions in the Digital Services Act (2022/2065), which exempts mere conduit, caching and hosting service providers from liability exposure in certain scenarios though also imposes additional due diligence obligations on providers of those services. The relationship between the GDPR, the E-commerce Directive, the Digital Services Act, and other of the EU's *"Big 5"* new data laws (the the Digital Markets Act, the Data Governance Act, the Data Act and the AI Act) is not straightforward. The Big 5 say that they are *"without prejudice*" to the application of the GDPR and in places stress that protection in regard to the processing of personal data is *"governed solely*" by data protection legislation. However, the Big 5 also contain a number of provisions which directly

relate to data protection (for example, the Digital Services Act's prohibition on profiling for advertising purposes based on minors'/ special category data in certain scenarios) and so in practice enforcement may feasibly arise under multiple acts. In certain other areas however the split is clearer (for example, the liability of ISPs for illegal content will likely continue to be enforced under the Digital Services Act, similarly to under the E-commerce Directive). Organisations should note that the Big 5 apply to both personal and non-personal data, and in places create rights like data subject rights under GDPR in respect of non-personal data too.

Organisations should be prepared to significantly expand their compliance programmes to deal with Big 5 compliance.

Regulation versus national law

As a Regulation, the GDPR is directly effective in Member States without the need for implementing legislation.

However, on numerous occasions, the GDPR does allow Member States to legislate on data protection matters. This includes occasions where the processing of personal data is required to comply with a legal obligation, relates to a public interest task or is carried out by a body with official authority. Numerous articles of the GDPR also state that their provisions may be further specified or restricted by Member State law. Processing of employee data is another significant area where Member States can take divergent approaches.

Organisations working in sectors where special rules often apply (e.g. health and financial services) should: (1) consider if they benefit from such *"special rules"* to the extent they have been introduced in relevant jurisdictions in order to particularise or liberalise the GDPR; and (2) adapt accordingly.

Where can I find this?

Material Scope, Article 2, Recitals 15-21
Territorial Scope, Article 3, Recitals 22-25

Key concepts for businesses to consider

At a glance

The following are key concepts under the GDPR which should form the basis of businesses' compliance programme structures:

- *Transparency and Consent* – the GDPR's stringent requirements regarding information to be provided and permissions required from individuals, including for consent to be unambiguous and not to be assumed from inaction, mean that many data protection notices, consent forms and "cookie consent banners" require additional disclosures or more granular levels of consent than in other jurisdictions.

- *Children's privacy*– given the focus on online safety, a number of European regulators have released specific guidance around how online services can comply with the GDPR specifically in relation to processing of children's data and there have been significant fines in this area. In addition, where online/Internet-enabled services rely on consent as a legal basis for processing, they need to check ages and ask for verifiable parental consent if the user is younger than a legally-specified age threshold (the "*age of digital consent*" – 16 by default, though some Member States have lowered it to 13, 14 or 15).

- *Regulated data* – the definitions of *"personal data"* and *"special categories of data"* are broad. In particular, regulatory guidance and case law suggests that *"anonymous"* data (which will not qualify as personal data) will be a very difficult standard to reach in practice, though regulatory attitudes vary by jurisdiction.

- *Pseudonymisation* – a privacy-enhancing technique where information which allows data to be attributed to a specific person is held separately and subject to technical and organisational measures to ensure non-attribution.

- *Personal Data Breach* – reporting obligations apply to all data controllers and all processors, regardless of their sector. (Telco providers are subject to breach notification obligations provided by the e-Privacy Directive).

- *Data protection by design and accountability* – organisations are required to adopt significant technical and organisational measures to comply and to be able to demonstrate their GDPR compliance.

- *Enhanced rights* – Data subjects are given substantial rights including the right to be forgotten, data portability rights and the right to not be subject to significant automated decision making.

- *Supervisory authorities and the EDPB* – regulatory oversight of data protection is on a national basis through a network of supervisory authorities, with the EDPB performing a co-ordination role. The EDPB also oversees the Article 65 dispute resolution process relating to enforcement around cross-border processing.

To do list

Refer to the *To do list* for later sections dealing with each of these topics in more detail

The GDPR's provisions and obligations are extensive, but the following are particularly key concepts which organisations should consider in their compliance programmes. More detailed information on each appears elsewhere in this guide.

Consent

The conditions for obtaining consent are strict:

- The Article 29 Working Party (now EDPB) stated in its GDPR consent guidelines that at least the following information is required for valid consent: (i) the controller's identity, (ii) the purpose of each of the processing operations for which consent is sought, (iii) what (type of) data will be collected and used, (iv) the existence of the right to withdraw consent, (v) information about the use of the data for automated decision-making in accordance with Article 22 (2)(c) where relevant, and (vi) the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46.
- There is a presumption that consent will not be valid unless: (i) separate consents are obtained for different processing activities, (ii) consent is not a condition of receiving a service, and (iii) there is no *"imbalance of power"* between the data subject and the organisation.

Consent is not the only mechanism for justifying the processing of personal data as the other legal bases available are contractual necessity, compliance with a (Member State or EU) legal obligation, or processing necessary for legitimate interests, protecting vital interests, or processing in the public interest.

For more information on this topic, see sections on consent; children; and special categories of data and lawful processing (see the section on principles).

Transparency

Organisations need to provide extensive information to individuals about the processing of their personal data. Breach of transparency obligations by controllers has led to some of the highest fines to date under the GDPR.

The list of information that must be provided takes up several pages in the GDPR; yet data controllers are nevertheless required to provide that information in a concise, transparent, intelligible and easily accessible way. The use of *"layered"* notices (with links to extra information) is a common solution, although some regulators (such as the Irish Data Protection Commissioner *("IDPC")* in its decisions against Meta's Instagram and Facebook processing) have noted that layering will *not* aid compliance to the extent it results in information overload for data subjects. The IDPC has also suggested (see separate decision in respect of WhatsApp's transparency practices, currently under appeal) that organisations will be expected to *"link"* together certain types of information in their privacy notices (for example, categories of data, purpose, lawful basis, and third party recipients). Many controllers have started to do this by using a table format.

Organisations are discouraged from making use of *"dark patterns"* to manipulate the user into making detrimental privacy choices. The EDPB issued guidelines on dark patterns which were

published in final form in 2023. There is a similar prohibition on online platforms' use of dark patterns in the Digital Services Act, but this will not apply to practices covered by the GDPR.

The transparency information of services *"likely to be accessed by children"* is held to a higher standard by European data protection regulators.

Where relevant, organisations are expected to implement privacy notices appropriate to the age of the children who access them, which might involve (for example) utilising video, audio, graphics, and/or simplified language.

For more information on this topic, see section on information notices.

Children

Children's privacy guidance

The online safety of minors has become a highly debated topic both in Europe and worldwide since the implementation of the GDPR. As such, a number of European supervisory authorities have taken action in this area and have issued specific guidance around the processing of children's data.

Examples include the UK Information Commissioner's Children's Code, and the Irish Data Protection Commissioner's Fundamentals for a Child-Oriented Approach to Data Processing. Topics focus on service design and include transparency, age assurance, default settings and *"nudge"* techniques.

Organisations will not only have to comply with children's privacy guidance if they directly target children with their services, but also if their services are *"likely to be accessed"* by children. Organisations will likely need to perform child accessibility assessments at the outset of designing their online services.

There have been substantial fines based on breaches of children's privacy guidance to date. For example, in 2022 the IDPC fined Meta 405 million Euros for making children's contact details public by default in breach of the GDPR.

The age of digital consent

In addition (and an overlapping but separate point to the children's privacy design guidance) children under the age of 13 can never, themselves, give consent to the processing of their personal data in relation to online/Internet-enabled services.

Therefore, for children between the ages of 13 and 15 (inclusive), the general rule is that if an organisation seeks consent as a GDPR legal basis to process their personal data, then parental consent must be obtained, unless the relevant Member State legislates to reduce the default age threshold (16 years of age). They cannot lower it below 13. Children aged 16 or older may give consent for the processing of their personal data themselves.

It should be noted however that consent is not the only lawful basis available for the processing of children's personal data. For example, it may still be possible for controllers of online services to rely on contract or legitimate interest where appropriate. However, it might be more difficult to reach the required threshold for other legal bases where children are concerned – for example, it might be more difficult to satisfy a legitimate interests assessment.

There are no specific rules relating to parental consent for offline data processing: usual Member State rules on capacity would apply here.

For more information on this topic, see section on children.

Personal data/ sensitive data ("Special categories of data")

The GDPR applies to data which can be related to a living individual that is identified or identifiable, whether directly or indirectly. Identifiability will be assessed taking into account *"all means reasonably likely to be used"* . Pre-GDPR, the CJEU's October 2016 ruling in *Patrick Breyer v Germany* (C-582/14) ("*Breyer*") confirmed that an individual will *not* be identifiable where the risk of identification *"appears in reality to be insignificant"*.

Regulatory guidance differs as to whether identifiability should be assessed from the perspective of anyone in the world, or solely from the perspective of the party seeking to consider the data anonymous. *Breyer* as well as General Court Case T-557/20 appear to favour the latter interpretation. Whether data *"relates to"* a natural person will depend on whether it is linked to that person by reason of its *"content, purpose or effect"* (*Peter Nowak v Data Protection Commissioner,* C-434/16 [2017], [35]), which is a low bar and likely to be satisfied if an individual is identifiable.

The GDPR's recitals highlight that certain categories of online data may be personal – for instance, data consisting of or associated with online identifiers, device identifiers, cookie IDs and IP addresses are given as examples. We have known since *Breyer* that a dynamic IP address can be personal data; Recital 30 GDPR reinforces the point.

"Special categories of data" (often referred to as sensitive data) include genetic data and biometric data used to identify data subjects. Processing of special categories of data is subject to more stringent conditions.

Pseudonymisation

Pseudonymisation refers to the technique of processing personal data in such a way that it can no longer be attributed to a specific *"data subject"* without the use of additional information, which must be kept separately and be subject to technical and organisational measures to ensure non-attribution.

Pseudonymised information is still a form of personal data, but the use of pseudonymisation is encouraged, for instance:

- it is a factor to be considered when determining if processing is *"incompatible"* with the purposes for which the personal data was originally collected and processed;
- it is included as an example of a technique which may satisfy requirements to implement *"privacy by design and by default"* (see section on data governance obligations);
- it may contribute to meeting the GDPR's data security obligations (see section on personal data breaches and notification); and
- for organisations wishing to use personal data for historical or scientific research or for statistical purposes, use of pseudonymous data is emphasised.

Personal data breach notification

The GDPR has a personal data breach notification framework for all data controllers (and all processors) regardless of the sector in which they operate. Some organisations (mainly telco providers) are subject to breach notification obligations provided by the e-Privacy Directive.

Notification obligations (to supervisory authorities and possibly to affected data subjects) are potentially triggered by *"accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data".* For more information on this topic, see section on personal data breaches and notification.

Data protection by design and accountability

Organisations must be able to demonstrate their compliance with the GDPR's principles, including by adopting certain *"data protection by design"* measures (e.g. the use of pseudonymisation techniques), staff training programmes and adopting policies and procedures.

Where *"high risk"* processing will take place (such as monitoring activities, systematic evaluations or processing special categories of data), a detailed data protection impact assessment (*"DPIA"*) must be carried out and documented. Where a DPIA results in the conclusion that there is indeed a high, and unmitigated, risk for the data subjects, controllers must notify the supervisory authority (i.e. the data protection authority or *"DPA"*) and obtain its view on the adequacy of the measures proposed by the DPIA to reduce the risks of processing.

Controllers and processors may decide to appoint a Data Protection Officer (*"DPO"*). This is obligatory for public sector bodies, those involved in certain listed sensitive processing or monitoring activities or where local law requires an appointment to be made. Group companies can jointly appoint a DPO.

For more information on these topics see section on data governance obligations.

Enhanced rights for individuals

The GDPR provides for a wide range of rights for individuals in respect of their personal data.

These include the right to be forgotten, the right to request the porting of one's personal data to a new organisation, the right to object to certain processing activities and an individual's right not to be subject to a decision based solely on automated processing which produces legal or other significant effects on him/her.

For more information on these topics see section on information notices and the immediately following sections.

The Data Governance Act *("DGA")* anticipates intermediary services, which will seek to help data subjects exercise their rights and give organisations access to their data. Those providing data intermediation services must meet conditions set out in the DGA, which are designed to ensure that the services are fair and independent. They must also act in the best interests of data subjects (DGA, Article12).

Supervisory authorities and the EDPB

Data protection regulators are referred to as supervisory authorities. A single lead supervisory authority located in the Member State in which an organisation has its *"main"* establishment will take the lead on cross-border complaints and investigations into that organisation's compliance with the GDPR.

The EDPB exists to (amongst many other things) issue opinions on particular issues and adjudicate on disputes arising from supervisory authority decisions under the Article 65 dispute resolution process.

For more information on this topic see Section 6: Regulators.

Data protection principles

At a glance

- The data protection principles are the building blocks of the wider GDPR. The principles underpin the specific obligations on controllers that follow in later chapters. This includes an accountability principle, requiring controllers to demonstrate how these principles are met by their processing.

To do list

- [ ] Identify means to *"demonstrate compliance"* with the data protection principles – e.g. adherence to approved codes of conduct, *"trails"* of decisions relating to data processing and, where appropriate, privacy impact assessments.

Commentary

The principles are the foundational building blocks of the GDPR, upon which later obligations on controllers are based. They are as follows:

Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.

Purpose limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

Further processing of personal data for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes is deemed to be compatible with the original processing purposes, if conditions in Article 89(1) (which sets out safeguards and derogations in relation to processing for such purposes) are satisfied.

Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Accuracy

Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay (having regard to the purposes for which the data is processed).

Storage limitation

Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1), *i.e.* subject to use of appropriate technical and organisational measures, which some Member States have addressed in national laws.

Integrity and confidentiality

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability

A controller is responsible for and must be able to demonstrate compliance with these principles.

Principles and enforcement

Principles are regularly referenced by supervisory authorities as part of enforcement action. Although certain obligations are subject to a lower penalty threshold under Article 83(4) GDPR, all breaches of the principles fall under the higher threshold under Article 83(5).

Where can I find this?

Article 5 and Recital 39

Lawfulness of processing and further processing

At a glance

- The GDPR sets out various grounds to lawfully process personal data under Article 6. These include consent, contractual necessity, legitimate interests, and legal obligations among others.
- The requirements for valid consent are onerous, and additional rules apply to the processing of children's data online.
- There are specific restrictions on the ability to rely on "legitimate interests" as a basis for processing, particularly in the public sector.
- There is a non-exhaustive list of factors to be taken into account when determining whether the processing of personal data for a new purpose is incompatible with the purposes for which the personal data was initially collected.

To do list

- [ ] Ensure you are clear about the grounds for lawful processing relied on by your organisation under the GDPR and that these are documented in your privacy notices.
- [ ] Where relying on consent, ensure the quality of that consent meets GDPR requirements (see the section on consent for further details).
- [ ] Ensure that your internal governance processes will enable you to demonstrate how decisions to use personal data for further processing purposes have been reached and that relevant factors have been considered.

Commentary

In order for the processing of personal data to be valid under the GDPR, data controllers must satisfy a condition set out in Article 6(1) GDPR (an additional legal basis is required to process special categories of data, over and above a legal basis in Article 6 – see the section on special categories of data and lawful processing). The relevant legal basis for each purpose of processing must be described in notices (see our section on information notices). As explained in the sections on data subject rights, individuals may have different rights depending on the legal basis relied upon for the processing. These legal bases for processing are:

6(1)(a) – Consent of the data subject

The GDPR test for valid consent is onerous, and sets a high bar for data controllers (see the section on consent). Particular conditions are also imposed where consent of children is sought online (see the section on children).

6(1)(b) – Necessary for the performance of a contract with the data subject or to take steps preparatory to such a contract

Processing must be necessary for the entry into or performance of a contract with the data subject. This is a preferable legal basis, where available, given the additional rights available to data subjects where controllers rely on consent or legitimate interests.

In October 2019, the EDPB issued its final guidelines on the processing of personal data under Article 6(1)(b) in the context of the provision of online services to data subjects. On the scope of this condition, the EDPB states that *"[m]erely referencing or mentioning data processing in a contract is not enough it is important to assess what is objectively necessary to perform the contract"*.

6(1)(c) – Necessary for compliance with a legal obligation

Article 6(3) and Recitals 41 and 45 make it clear that the legal obligation in question must be:

- an obligation of Member State or EU law to which the controller is subject; and
- *"clear and precise"* and its application foreseeable for those subject to it.

The recitals make it clear that the relevant *"legal obligation"* need not be statutory (i.e. common law would be sufficient, if this meets the *"clear and precise"* test). A legal obligation could cover several processing operations carried out by the controller so that it may not be necessary to identify a specific legal obligation for each individual processing activity.

6(1)(d) – Necessary to protect the vital interests of a data subject or another person where the data subject is incapable of giving consent

Recital 46 suggests that this legal basis is available for processing that is necessary for humanitarian purposes (e.g. monitoring epidemics) or in connection with humanitarian emergencies (e.g. disaster response). The recital indicates that in cases where personal data is processed in the vital interests of a person other than the data subject, this legal basis for processing should be relied on by exception, and only where no other legal basis is available.

6(1)(e) – Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

Article 6(3) and Recital 45 make clear that this legal basis applies only where the task carried out, or the authority of the controller, is laid down in Union law or Member State law to which the controller is subject. This is the key alternative for public authorities, who are not able to process personal data for their public tasks on the basis of legitimate interests.

6(1)(f) – Necessary for the purposes of legitimate interests

As set out above, this legal basis can no longer be relied on by public authorities processing personal data in the exercise of their functions. Recitals 47-50 add more detail on what may be considered a *"legitimate interest"*. Guidance from the EDPB makes it clear that a documented balancing test (also called a legitimate interests assessment or *"LIA"*) is expected where relying on this legal basis, which must be made available to data subjects on request (see the section on legitimate interests for further details).

Member States are permitted to introduce specific provisions to provide a basis under Articles 6(1)(c) and 6(1)(e) (processing due to

a legal obligation or performance of a task in the public interest or in the exercise of official authority). This has led to some variation across the EU. (For further details see the section on derogations and special conditions).

The lawful bases that online platforms rely on to process personal data have been considered by the CJEU and the EDPB. In the *Bundeskartellamt* decision (C-252-121), the CJEU suggested a narrow interpretation of contractual necessity, noting that it would cover processing which was *"objectively indispensable"* for the main subject matter of the contract, and of legitimate interests-based processing. However, the CJEU noted that the fact that a platform has a dominant position does not preclude it from relying on user consent.

In its Binding Decision 03/2022, the EDPB directed the IDPC to find that performance of a contract was not a suitable legal basis on which Meta could rely to process personal data of users for targeted advertising. On 7th December 2023, the EDPB adopted an urgent binding decision on this topic, relating to use of performance of a contract and legitimate interests for processing of certain data for targeted advertising.

Additional considerations on lawful basis apply under the Digital Markets Act *("DMA")*. The DMA is only applicable to a small number of very large gatekeepers (listed here: Gatekeepers (europa.eu)). The European Commission designates gatekeepers in respect of specific services. Article 5 DMA prohibits gatekeepers from carrying out certain processing of personal data unless the gatekeeper has the consent of the data subject – so, for these specific processing activities, gatekeepers have less flexibility on lawful basis than other controllers. The restrictions apply to:

- processing personal data of end users for online advertising services, where the personal data relates to end-user's interactions with third parties who use the gatekeeper's services;
- combining personal data from a regulated service with personal data from other services;
- cross-using personal data from a regulated service with personal data from other services; and
- signing end-users in to other services of the gatekeeper in order to combine personal data.

If the processing listed above is required by (EU or member state) law, to protect vital interests, or for a task performed in the public interest, then the gatekeeper can still go ahead.

Further processing

The GDPR also sets out (at Article 6(4)) the factors a controller must take into account to assess whether a new processing purpose is compatible with the purpose for which the personal data was initially collected. Where such processing is not based on consent, or on Union or Member State law relating to matters specified in Article 23 (general article on restrictions relating to the protection of national security, criminal investigations etc.), the following factors should be taken into account in order to determine compatibility:

- any link between the original and proposed new purposes;
- the context in which personal data have been collected (in particular the relationship between data subjects and the controller);
- the nature of the personal data (particularly whether they are special categories of data or criminal offence and convictions data);
- the possible consequences of the proposed processing; and
- the existence of safeguards (including encryption or pseudonymisation).

Recital 50 and Article 5(1)(b) indicate that further processing for archiving purposes in the public interest, for scientific and historical research purposes or for statistical purposes should be considered as compatible processing (see the section on derogations and special conditions).

Impact of new EU laws

There are restrictions on the ability of organisations who receive personal data under the Data Act to make further use of this data. The Data Act enhances the right to portability, by allowing end-users better access to data generated by connected devices and related services. The end-user can direct that this data should be made available to a third party – for example, so that the third party can provide support or after-care services related to the connected device to the end-user. Where third parties receive connected device data under the Data Act, then Article 6 Data Act imposes stricter purpose limitation restrictions on the third party. The third party can only use the data for the purposes and under the conditions agreed with the user of the device. The third party is also not allowed to share the data with another third party unless this sharing is also on the basis of a contract with the end-user. This means that a third party who has received personal (or other) data under the Data Act is not able to make further, compatible, use of the data; the third party can only use the data for the original purpose for which it was provided.

Further Reading:

- EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects
- *C-268/21 Norra Stockholm Bygg* addresses Articles 6(1)(e), 6(3) and 6(4) in the context of civil disclosure.
- European Commission published in April 2019 a Q&A document looking into the interplay between the EU Clinical Trial Regulation and the GDPR, addressing further processing.
- C-77/21 DIGI addresses further processing, explaining the need for a "concrete, logical and sufficiently close link" between the initial and further processing, not deviating from the individual's "legitimate expectation"
- IDPC decisions against Meta which address the ability to rely on contractual necessity

Where can I find this?

Lawful basis for processing (personal data)
Articles 6-10, Recitals 40-50

Legitimate interests

At a glance

- Legitimate interests is the most flexible legal basis for most data controllers.
- The legitimate interest may be that pursued by the controller or a third party, but must not be overridden by the interests or fundamental rights or freedoms of the data subject, in particular where that individual is a child.
- Public authorities are unable to rely on legitimate interests to legitimise data processing carried out in the discharge of their functions.
- Controllers that rely on legitimate interests should maintain a record of the assessment they have made (i.e. an LIA). EDPB guidance states that this assessment should be provided to data subjects on request, and that individuals should be told that they have this right. This assessment will also be necessary to help controllers show that they have given proper consideration to the rights and freedoms of data subjects.
- Controllers should be aware that persona data processed on the basis of legitimate interests is subject to a right to object – which can only be rejected where there are *"compelling"* reasons.

To do list

- [ ] Ensure you have identified the relevant legal basis for processing your organisation's personal data, and have documented this internally and in information notices.
- [ ] If your organisation is a public authority, ensure you have identified another legal basis for the processing of personal data for your public functions (e.g. processing necessary in the public interest or in the exercise of official authority).
- [ ] Where legitimate interests are relied on, ensure that the relevant legitimate interest is identified in the information that must be supplied to data subjects pursuant to Articles 13 and 14 (see the section on information notices).
- [ ] Where relying on legitimate interests, ensure that decision-making in relation to the balance between the interests of the controller (or relevant third party) and the rights of data subjects is documented in an LIA and that this is available to be shared with data subjects where requested. Ensure your information notices tell people of this right.

Commentary

Article 6(1) GDPR states that personal data processing shall be lawful only where at least one of the provisions at Article 6(1) (a)-(f) applies.

Article 6(1)(f) applies where:

"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

Article 6(1) makes clear that subsection (f) shall not apply to *"processing carried out by public authorities in the performance of their tasks".* This said, legitimate interests can still be relevant to public authorities to the extent that their processing is for a purpose outside of their public task. Additionally, the need to specifically consider the interests and rights of children is also new (see the section on children).

In practice, the major considerations for organisations when they rely on legitimate interests under the GDPR relate to accountability (the need to carry out and record the balancing test via an LIA) and to the rights of data subjects attached to this condition for processing (including rights to notice and to object).

What are legitimate interests?

The recitals to the GDPR give examples of processing that could be necessary for the legitimate interest of a data controller. These include:

- Recital 47: processing for direct marketing purposes or preventing fraud;
- Recital 48: transmission of personal data within a group of undertakings for internal administrative purposes, including client and employee data (note that international transfer requirements will still apply – see the section on transfer of personal data);
- Recital 49: processing for the purposes of ensuring network and information security, including preventing access to electronic communications networks and stopping damage to computer and electronic communication systems; and
- Recital 50: reporting possible criminal acts or threats to public security to a competent authority.

Recital 47 also states that controllers should consider the expectations of data subjects when assessing whether their (i.e. the controllers') legitimate interests are outweighed by the interests of data subjects. The interests and fundamental rights of data subjects *"could in particular override"* that of the controller where data subjects *"do not reasonably expect further processing".*

Recital 47 also sets out that controllers are expected *"at any rate"* to carry out a *"careful assessment"* to determine whether there is a legitimate interest. In order to comply with the accountability principle, controllers should document this assessment or *"balancing test"* in an LIA. According to the CJEU, this is a three part test, as set out in the *Valsts policijas Rigas regiona parvaldes Kartibas policijas parvalde v Rigas pašvaldibas SIA 'Rigas satiksme* (C13/16) case:

- identifying the relevant interests;
- determining if the processing is necessary; and
- balancing this with the interests of the individual.

Information notices must set out legitimate interests – and potentially how to access details of balancing tests

Where legitimate interests are relied on in relation to specific processing operations, this will need to be set out in relevant information notices, by virtue of Articles 13 (1)(d) and 14 (2)(b).

The EDPB guidance on transparency expands on this requirement: *"as a matter of best practice, the controller can also provide the data subject with the information from the balancing test which must be carried out to allow reliance on Article 6.1(f)[...] In any case, the [Article 29 Working Party] position is that information to the data subject should make it clear that they can obtain information on the balancing test upon request"*.

Controllers need to ensure that they specifically name the relevant legitimate interests they rely upon in their information notices, and consider telling individuals about their right to access balancing tests at the same time. Although not

specifically named as an obligation in the GDPR itself, the EDPB guidance states that doing so is considered *"essential for effective transparency*".

Specific right to object

Data subjects are able to object to processing based on legitimate interests, although they must demonstrate that this is based on *"grounds relating to his or her particular situation"*. The burden then lies on data controllers to prove that they have compelling grounds to continue processing the data. This right to object can lead to the exercise of rights to restrict and erase data (see the section on rights to object for more information).

Check for Codes of Conduct

Article 40 requires Member States, supervisory authorities, the EDPB and the European Commission to encourage the creation of codes of conduct in relation to a wide range of subjects including the legitimate interests pursued by data controllers in specific contexts. Whilst limited progress has been made on this to date, members of trade associations or similar sector specific bodies should watch for the creation of such codes, which might impose particular additional requirements.

Data transfers – a new ground, but unlikely to ever be of use in practice

A final outing for legitimate interests comes in Article 49(1), which states that transfers can be made based on *"compelling legitimate interests"* where they are not repetitive, relate to only a limited number of data subjects and where the controller has assessed and ensured adequacy. However, this ground can only be used where the controller cannot rely on any other method of ensuring adequacy, including model clauses, binding corporate rules *("BCRs")*, approved contracts and all derogations under Article 49(1)(a)-(f). As set out in EDPB guidance on the derogations under Article 49, *"this derogation is envisaged by the law as a last resort"*. The controller would then need to notify the supervisory authority that it was relying on this ground for transfer – although the EDPB guidance recognises that this is not a need to seek authorisation.

Further Reading:

- EDPB Guidelines 8/2020 on the targeting of social media users
- EDPB Guidelines expected on legitimate interests in 2024-2025 EDPB work programme
- EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679
- IDPC decisions against Meta which address legitimate interest as a lawful basis
- IDPC decision against WhatsApp on the level of information required on legitimate interests in privacy notices.
- Forthcoming CJEU case C-621/22 will investigate the ability to rely on solely commercial legitimate interests (which has been narrowly approached by the Dutch DPA).

Where can I find this?

Legitimate Interests
Articles 6(1)(f), 13(1)(d), 14(2)(b) and 49(1)
Recitals 47, 48, 49, 50

Consent

At a glance

- Consent has strict validity requirements under the GDPR
- Consent must be a "*freely given, specific, informed and unambiguous indication of the data subject's agreement* ". In practice this requires that consent be truly voluntary, separate from other consent requests, actively communicated, and as easily withdrawn as given. These requirements are often hard to meet in practice.
- Specific rules also apply to children in relation to information society services, where parental consent may be required

To do list

☑ Ensure you are clear about the legal basis for lawful processing relied on by your organisation.

☑ Consider whether rules on children online affect you, and, if so, which national rules you need to follow when obtaining consent (see section on children for further details).

☑ If your organisation relies on consent to process personal data for the purpose of scientific research, consider offering data subjects the opportunity to consent only to certain areas of research or parts of research projects. Also consider national research derogations as an alternative (see section on derogations and special conditions).

☑ Where relying on consent as the basis for lawful processing, ensure that:

- consent is active, and does not rely on silence, inactivity or pre-ticked boxes;
- consent to processing is distinguishable, clear, and is not bundled with other written agreements or declarations;
- supply of services is not made contingent on consent to processing which is not necessary for the service being supplied (outside limited permitted situations, see below);
- data subjects are informed that they have the right to withhold or withdraw consent at any time without detriment but that this will not affect the lawfulness of processing based on consent before its withdrawal;
- there are simple methods for withdrawing consent, including methods using the same medium used to obtain consent in the first place;
- separate consents are obtained for distinct processing operations; and
- consent is not relied on where there is a clear imbalance between the data subject and the controller (especially if the controller is a public authority).

Commentary

What is consent, what is an unambiguous indication of wishes and when is it needed?

Article 4(11) GDPR defines *"the consent of the data subject"* as *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".*

Consent is one of a number of legal bases for processing permitted under Article 6 GDPR (see section on lawfulness of processing and further processing).

Recital 32 suggests that an unambiguous indication of wishes may be signified by:

"ticking a box when visiting a... website, choosing technical settings... or by any other statement or conduct which clearly indicates... the data subject's acceptance of the proposed processing of their personal data. Silence, pre-ticked boxes or inactivity should therefore not constitute consent."

The EDPB has produced consent guidance that additionally clarifies *"the use of pre-ticked opt-in boxes is invalid under the GDPR. Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice".*

Explicit consent is still required to justify the processing of special categories of data unless other grounds apply (on which see the section on special categories of data and lawful processing). In addition, explicit consent, in the absence of adequacy or other conditions, can be relied on under the GDPR for the transfer of personal data outside the EU (see section on transfers of personal data) and as one of the legal bases for the making of significant automated decisions relating to an individual (see section on profiling and automated decision-taking).

Steps to validity – specified, informed, distinguishable, revocable, granular and otherwise freely given

Article 7(1) GDPR requires that where consent is relied on as a ground for lawful processing, controllers should be able to demonstrate that consent was given by the data subject to the processing. The rest of Article 7 is dedicated to setting out the conditions for a valid consent.

These are:

- Article 7(2): Consent to processing contained in a written declaration produced by the controller must be distinguishable from other matters in that declaration, intelligible, easily accessible and be in clear and plain language. Recital 42 cites the Unfair Terms in Consumer Contracts Directive (Directive 93/13/EEC) as the inspiration for these obligations. In practice, this will require consent to processing to be clearly distinguishable within broader contracts or agreements.

- Recital 42 also notes that consent will be informed only where the data subject is aware of (at least) the identity of the controller and the intended purposes of processing. This is supplemented by EDPB guidance on consent, which says that additionally individuals must know what (type of) data will be collected and used, the existence of the right to withdraw consent, information about the use of automated processing techniques which have legal or similarly significant effect and (if the consent relates to transfers of data outside the EEA) information about the possible risks of data transfers to third countries. All the above elements must appear (if relevant) in the text of the consent mechanism itself.

- Article 7(3): This provision further explains that data subjects must have the right to revoke their consent at any time, and it must be as easy to withdraw consent as it is to give it. In practice, at a minimum this is likely to require organisations to allow consent to be withdrawn through the same medium (e.g. website, email, text) as it was obtained (the EDPB in its consent guidelines stated that where obtained through a particular electronic interface, there is *"no doubt a data subject must be able to withdraw consent via the same electronic interface, as switching to another interface for the sole reason of withdrawing consent would require undue effort"*). The GDPR acknowledges that the withdrawal of consent does not retrospectively render processing unlawful, and processing can continue on another legal basis if appropriate but this requires the controller to inform data subjects of this before consent is given. The EDPB emphasised *"controllers have an obligation to delete data that was processed on the basis of consent once that consent is withdrawn, assuming that there is no other purpose justifying the continued retention".*

- Article 7(4): Where the performance of a contract, including the provision of a service, is made conditional on consent to the processing of persona data that is not necessary for the performance of that contract, this is likely to call into question the extent to which consent can be considered to be freely given. As a result, the provision of a service should not be made contingent upon the data subject's consent to the processing of their data for purposes that are unnecessary for the provision of the service.

- The EDPB guidance on consent confirms that "*the element "free" implies real choice and control for data subjects*" and "*any element of inappropriate pressure or influence upon the data subject (which may be manifested in many different ways) which prevents a data subject from exercising their free will, shall render the consent invalid*".

Recital 43 GDPR indicates that consent will be presumed not to be freely given if:

- despite it being appropriate in the circumstances, there is no provision for separate consent to be given to different processing operations; or

- *"the performance of a contract, including the provision of a service, is dependent on the consent, despite such consent not being necessary for such performance."*

This is a requirement to ensure granularity of consent. The EDPB guidance warns that *"if the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom."* Controllers should take care not to combine multiple processing purposes into a single consent.

Recital 43 also notes that imbalance of power between the parties can lead to consent being considered invalid and not freely given. This Recital specifically points to this being likely in the case where the controller is a public authority.

Another example is also given by the EDPB consent guidelines in relation to employers: *"given the imbalance of power between an employer and its staff members, employees can only give free consent in exceptional circumstances, when it will have no adverse consequences at all whether or not they give consent*".

Finally, Recital 42 states that *"consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment".* The EDPB consent guidance discusses detriment at some length, stating that the GDPR does not *"preclude all incentives"* but that individuals must be able to withdraw or withhold consent without incurring cost or "*clear disadvantage*". Despite the absence of opposition from the EDPB on the question of incentivisation, it should be noted that certain supervisory authorities in Member States are clearly opposed to such techniques (e.g. the CNIL in France) whereas others (e.g. in Denmark and Finland) have concluded that this may permit organisations to make competitions or loyalty scheme memberships contingent on consent to marketing (see further reading).

Children and research

Specific conditions apply to the validity of consent given by children in relation to information society services, with requirements to obtain and verify parental consent below certain age limits (see the section on children for further details).

Recital 33 GDPR addresses consent that is obtained for scientific research purposes. It acknowledges that *"it is often not possible to fully identify the purpose of data processing for scientific research purposes at the time of data collection"* and states that:

- data subjects should be able to consent to certain areas of scientific research, where this meets *"ethical standards"* for such research; and

- data subjects should be able to grant consent only to *"certain areas... or parts of research projects to the extent allowed by the intended purpose".*

The EDPB guidance on consent emphasises that it is important that *"consent for the use of personal data should be distinguished from other consent requirements that serve as an ethical standard or procedural obligation".* There remains much ongoing debate as to the most appropriate legal basis for research, and the potential for relying on a pre-existing legal basis for further processing (see the section lawfulness of processing and further processing).

Language of consent

The GDPR requires that consent be intelligible, informed and unambiguous. The EDPB guidelines on consent emphasise that *"when seeking consent, controllers should ensure that*

they use clear and plain language in all cases. This means a message should be easily understandable for the average person and not only for lawyers". It is also unlikely that consent will meet these requirements if the consent is in a foreign language incomprehensible to the individual.

New EU laws

The DMA imposes additional restrictions on consent. Article 5 DMA provides that if the data subject refuses or withdraws consent, the gatekeeper cannot repeat its request for consent for that same purpose that same year.

Further Reading:

- EDPB Guidelines 8/2020 on the targeting of social media users
- EDPB Guidelines 5/2020 on consent
- EDPB Guidelines 3/2022 on dark patterns in social media platform interfaces
- Decisions by the Danish DPA and Finnish DPA on incentivizing consent
- CJEU case C-673/17 *Planet 49* (consent must be active and cannot be sought through pre-checked boxes)
- EDPB Cookie Banner Taskforce report
- CJEU case C-252/21 addressing whether consent can be freely given to a dominant undertaking (Facebook/Instagram)

Where can I find this?

Articles 4(11), 6(1)(a), 7, 8 and 9(2(a))
Recitals 32, 33, 42 and 43

Children

At a glance

- There are a handful of child-specific provisions in the GDPR, particularly in relation to legal basis for processing and notices.
- Children are identified as *"vulnerable individuals"* and deserving of *"specific protection"*.
- Processing of data relating to children is noted to carry certain particular risks, and further restrictions may be imposed as a result of codes of conduct.
- Where online services are provided to a child and consent is relied on as the basis for the lawful processing of his or her data, consent must be given or authorised by a person with parental responsibility for the child. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit - which may be no lower than 13).
- Many national authorities have begun to adopt child-specific guidance, and further guidance is expected from the EDPB in 2024.

To do list

- [ ] Consider whether rules and guidance on children are likely to affect you.
- [ ] If your organisation offers information society services directly to children where consent is required, assess which national rules will apply and ensure that appropriate parental consent mechanisms are implemented, including verification processes.
- [ ] Remain aware of national legislation and guidance for offline data processing relating to children's data.
- [ ] Where processing data of children – whether targeted or not - ensure notices are drafted clearly with a child's understanding in mind.
- [ ] Ensure any reliance on *"legitimate interests"* to justify processing children's data is backed up with a careful and documented consideration of whether a child's interests override those of your organisation.

Commentary

The importance of protecting children is mentioned several times in the GDPR, and has been highlighted in EDPB guidance. In practice, the GDPR itself provides little harmonisation, and substantive restrictions come from national laws, compliance with EDPB guidance or codes of conduct (see the section on codes of conduct and certifications for further details).

Parental consent

The main provision in relation to children is Article 8, which requires parental consent to be obtained for information society services offered directly to a child under the age of 16 – although this ceiling can be set as low as 13 by a Member State, and only applies where the processing would be based on the child's consent. Member States have picked a wide range of ages, from Denmark, Belgium and others at the minimum of 13, Austria at 14, France and the Czech Republic at 15 and many such as the Netherlands and Ireland retaining an age of 16.

The controller is also required, under Article 8(2) GDPR, to make *"reasonable efforts"* to verify that consent has been given or authorised by the holder of parental responsibility in light of available technology.

This only affects certain online data – offline data will continue to remain subject to the usual Member State rules on capacity to consent. Article 8(1) is also not to be considered as affecting the general contract law of Member States regarding the validity, formation or effect of a contract with a child. Organisations will still need to consider local laws in this area.

Notices addressed to children must be child-friendly

Article 12 GDPR provides that the obligations to ensure that information provided to data subjects is concise, transparent and in plain language are to be met *"in particular for any information addressed specifically to a child"*. Recital 58 expands:

"Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand."

The GDPR recognises the UN Convention definition of a child as anyone under the age of 18. Controllers should therefore be prepared to address these requirements in notices directed at teenagers. The EDPB says that controllers should *"ensure that the vocabulary, tone and style of the language used is appropriate to and resonates with children."* The EDPB's guidance does at least recognise that "*with very young or pre-literate children, transparency measures may also be addressed to holders of parental responsibility given that such children will, in most cases, be unlikely to understand even the most basic written or non-written messages concerning transparency".*

Data Protection Impact Assessments – processing child data may contribute to processing being considered high risk in the circumstances

As discussed elsewhere in this guide, a DPIA must be carried out where a controller carries out high risk processing. EDPB guidance on DPIAs has noted that processing the data of vulnerable individuals – which include children - is one criterion that may, when considered with other factors, lead to a processing activity being high risk *"because of the increased power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights".*

Miscellaneous provisions – helplines, codes of conduct and work for supervisory authorities

Article 6(1)(f) GDPR notes that the rights and freedoms of a data subject may *"in particular"* override the interests of the controller or third party where the relevant data subject is a child. Controllers should ensure that clear documentation is kept demonstrating that relevant competing interests have been appropriately considered in a balancing test where relying on legitimate interests for processing data relating to children.

Recital 38 notes that the use of child data in marketing, or for profiling purposes or in connection with the supply of services to children are areas of concern requiring specific protection under the GDPR. The recital also states that parental consent should not be required in the context of preventative and/or counselling services offered directly to a child although this suggestion does not appear to be reflected in the articles of the GDPR itself.

Article 40 requires Member States, supervisory authorities, the EDPB and the European Commission to encourage the creation of codes of conduct, including in the area of the protection of children, and concerning the way in which consent can be collected from the holder of relevant parental responsibility. Organisations that process personal data relating to children should watch for the creation of such codes, which might impose particular additional requirements.

Since the UK's Information Commissioner published the Age Appropriate Design Code in January 2020, some Member States have adopted guidance on children's data processing, notably Ireland and France. The EDPB is also due to release Guidelines on processing of children's data as part of its 2023-2024 work programme.

Finally, supervisory authorities, when promoting public awareness and understanding of risks, rules, safeguards and rights in relation to the processing of personal data, pursuant to the obligation imposed on them by Article 57(1)(b), are required to give *"specific attention"* to activities addressed to children.

Where can I find this?

Articles 6(1)(f), 8, 12(1), 40(2)(g), 57(1)(b)
Recitals 38, 58, 75

Special categories of data and lawful processing

At a glance

- "*Special categories of personal data*" are data revealing "*racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*"
- The grounds permitting processing of special categories of data under the GDPR are narrow and specific. In a number of cases, these provisions still involve reliance on EU or Member State laws.
- There is also a broad ability for Member States to introduce new conditions (including limitations) regarding the processing of genetic, biometric or health data.

To do list

- [ ] Ensure you are clear about the grounds relied on by your organisation to process special categories of data and have considered the application of EU or Member State laws as necessary;
- [ ] Where relying on explicit consent, ensure the consent meets validity obligations (see the section on consent); and
- [ ] Ensure you have checked and continue to pay attention to national developments as Member States have a broad right to impose further conditions - including restrictions - on the grounds set out in the GDPR.

Commentary

Article 9(2) sets out the circumstances in which the processing of special categories of data, which is otherwise prohibited, may take place. These involve the following categories of data, as set out in Article 9(1):

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- data concerning health or sex life and sexual orientation;
- genetic data; and
- biometric data where processed to uniquely identify a person.

Recital 51 suggests that the processing of photographs will not automatically be considered as processing of biometric data (as had been the case in some Member States prior to GDPR); photographs or footage will be covered only to the extent they allow the unique identification or authentication of an individual (such as when used as part of an electronic passport).

In the *Bundeskartellamt* case (C-252/21) the CJEU concluded that if someone visits a website or app which relates to one of the special categories, and registers with the site or places an order, then that data will be special category data – including if it is automatically collected by a social network which interfaces with the site or app. The CJEU has also concluded that data about your partner (such as their name) can reveal information about an individual's sexual orientation (C-184/20).

The grounds for processing special categories are:

9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law

If relying on this ground, conditions for valid consent should be carefully considered (see the section on consent).

9(2)(b) – Necessary for the carrying out of obligations under employment, social security or social protection law, or a collective agreement

9(2)(c) – Necessary to protect the vital interests of a data subject who is physically or legally incapable of giving consent

9(2)(d) – Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent

9(2)(e) – Data manifestly made public by the data subject

9(2)(f) – Necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity

9(2) (g) – Necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguarding measures

This enables Member States to extend by law the circumstances where special categories of data may be processed in the public interest. In many countries this has required no change, where such provisions have remained in pre-existing legislation. In others, broad substantial public interest provisions exist in sectoral laws or in data protection legislation.

9(2)(h) – Necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

AND

9(2)(i) - Necessary for reasons of public interest in the area of public health, such as protecting against serious cross- border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices

These two provisions provide a formal legal justification for uses of healthcare data in the health and pharmaceutical sectors by providers of social care. It is important to remember that the first of these provisions does still require a basis under EU or local law, and both conditions require obligations of confidentiality to be in place as an additional safeguard.

9(2)(j) - necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

This makes provision for the processing of special categories of data for the purposes of archiving, research and statistics, subject to compliance with appropriate safeguards, including safeguards to ensure respect for the principle of data minimisation (see the section on derogations and special conditions for further details).

Genetic, biometric, or health data

Member States are also entitled, under Article 9(4) GDPR, to maintain or impose further conditions (including limitations) in respect of genetic, biometric or health data.

Criminal convictions and offences

Data relating to criminal convictions and offences are not categorised as a special category of data for the purposes of the GDPR. This is consistent with previous provisions as data of this kind was not treated as a special category of data under the Data Protection Directive.

Similarly, the rules under the GDPR in relation to data concerning criminal convictions and offences mirror those which applied under the Data Protection Directive. Article 10 provides that such data may be processed only under the control of official authority or where the processing is authorised by Union law or Member State law that provides appropriate safeguards. There is notable national divergence in this area.

Information notices

At a glance

- Controllers must provide information notices, to ensure transparency of processing.
- Specified information must be provided, and there is also a general transparency obligation.
- There is an emphasis on clear, concise notices.

To do list

- [ ] Audit existing information notices and review and update them.
- [ ] For data which is collected indirectly, ensure that notice is given at the appropriate time.
- [ ] Work with relevant partners who may collect data on your organisation's behalf to assign responsibility for notice review, update and approval.

Commentary

The principle of *"fair and transparent"* processing means that the controller must provide information to individuals about its processing of their data, unless the individual already has this information. The information to be provided is specified in the GDPR and listed below. The controller may also have to provide additional information if, in the specific circumstances and context, this is necessary for the processing to be fair and transparent.

The information must be provided in a concise, transparent, intelligible and easily accessible way, using clear and plain language (in particular where the data subject is a child).

What must a controller tell individuals?

Additional guidance from the former Article 29 Working Party ("*WP29*") on transparency is included below. Notably the former WP29's guidance goes further than the GDPR requirements on a number of fronts:

- Identity and contact details of the controller (or its representative, for a non-EU established controller); contact details of the Data Protection Officer. Guidance states the controller should also allow for different channels of communication (e.g. phone, email, postal address etc.).

- Purposes of processing and legal basis for processing – including the *"legitimate interest"* pursued by the controller (or third party) if this is the legal basis. Guidance states that that the purposes should be set out together with the relevant lawful basis relied on. This was confirmed by the EDPB binding decisions in relation to the Irish Data Protection Commissioner's fines against Meta relating to Facebook, Instagram and WhatsApp. It should also be made clear that the individual can obtain further information on the legitimate interest exercise on request (commonly abbreviated to LIA), where this information is not already set out in the information notice.

- Where special categories of data are processed, the lawful basis provided by Article 9 of the GDPR should be specified (and other EU or Member State law where relevant). Where criminal conviction and offence data are processed, the relevant EU or Member State law on which the processing is carried out should be noted.

- Recipients, or categories of recipients. According to the guidance, controllers must provide information on recipients which is most meaningful to the individual which will generally involve naming recipients. Recipients include controllers, joint controllers and processors. According to the guidelines, where a controller chooses to name only categories of recipients, this should be as specific as possible indicating the type of recipient, the industry, sector and sub-sector and the recipients' location.

- Details of data transfers outside the EU:

  – including how the data will be protected (e.g. the recipient is in an adequate country; Binding Corporate Rules are in place etc.); and

  – how the individual can obtain a copy of the BCRs or other safeguards, or where such safeguards have been made available.

  – According to the guidance, the relevant GDPR article permitting the transfer and the corresponding adequacy mechanism should be specified. Where possible, a link to the adequacy mechanism used or information on where the document may be accessed should be included. The information provided on transfers to third countries should also be as meaningful as possible to individuals; according to the guidance this will generally mean that third countries should be named.

- The retention period for the data – if not possible, then the criteria used to set this. According to the guidance it is not sufficient for the controller to generically state that data will be kept as long as necessary. Where relevant, the different storage periods should be stipulated for different categories of personal data and/or different processing purposes, including where appropriate, archiving periods.

- That the individual has a right to access and port data, to rectify, erase and restrict his or her personal data, to object to processing and, if processing is based on consent, to withdraw consent. According to the guidance where Member State implementing legislation qualify or restrict the data subjects' rights, the controller must notify individuals of any qualification to their rights which the controller may rely on.

- That the individual can complain to a supervisory authority.

- Whether there is a statutory or contractual requirement to provide the data, or a requirement to provide data in order to enter into a contract, and the consequences of not providing the data.

- If there will be any automated decision taking – together with information about the logic involved and the significance and consequences of the processing for the individual.

In case of indirect data collection activities, the controller must also tell individuals the categories of information and the source(s) of the information, including if it came from publicly accessible sources. According to the guidance, details should include the nature of the sources (i.e. publicly/privately held sources; the types of organization/industry/sector; and where the information was held (EU or non-EU).

The controller does not have to provide this information to the individual if it would be impossible or involve a disproportionate effort. In these cases, appropriate measures must be taken to protect individuals' interests and the information notice must be made publicly available.

There is also no need to provide the information notice:

- if there is an EU or member state law obligation for the controller to obtain/disclose the information; or

- if the information must remain confidential, because of professional or statutory secrecy obligations, regulated by EU or Member State law.

If the controller later processes personal data for a new purpose, not covered in the initial notice, then it must provide a new notice covering the new processing.

Providing all of this information is hard to reconcile with the GDPR's own requirement of conciseness and clarity. To help better achieve this, there is an ability for the European Commission to introduce standardised icons by means of delegated acts. If introduced, these would then also need to be displayed to individuals.

When must a controller provide this information?

Controller obtains information directly from individual

- At the time the data is obtained.

The controller must also tell individuals what information is mandatory and the consequences of not providing information.

Controller does not obtain information directly from individual

- Within a reasonable period of having obtained the data (max one month); or

- If the data are used to communicate with the individual, at the latest, when the first communication takes place; or

- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

Possible supplemental Member State disclosure requirements

In addition to the requirements provided by Articles 13 and 14 of the GDPR, certain Member States have added or maintained supplemental elements to be addressed in information notices. For instance, in France, information notices must indicate the existence of a right for data subjects to give instructions concerning the use and disclosure of their personal data after their death.

Updates to the information notice

According to the former Article 29 Working Party, controllers must take *"all measures"* necessary to bring specific changes to the individual's attention (such communications should also be separate from direct marketing content). The former Article 29 Working Party provided non-exhaustive examples of changes to an information notice which should always be communicated to an individual, these include: a change in the processing purpose, a change in the controller's identity, and changes as to how an individual can exercise their rights.

Further reading:

Article 29 Working Party Guidelines on transparency under Regulation 2016/679, endorsed by the EDPB

EDPB Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them

Irish DPC decisions against Meta Ireland (Facebook and Instagram)

EDPB Binding Decisions on the dispute submitted by the Irish SA on Meta Platforms, WhatsApp, Instagram and Facebook services

Where can I find this?

Articles 12-14
Recitals 58, 60, 61 and 62

Subject access, rectification and portability

At a glance

- Controllers must, on request:
  - confirm if they process an individual's personal data;
  - provide a copy of the data (in commonly used electronic form in many cases); and
  - provide supporting (and detailed) explanatory materials.
- Data subjects can also demand that their personal data be ported to them or to a new provider in machine readable format if the data in question was: 1) provided by the data subject to the controller (interpreted broadly); 2) is processed automatically; and 3) is processed based on consent or fulfilment of a contract.
- The request must be met within one month (with extensions for some cases) and any intention not to comply must be explained to the individual.
- Access rights are intended to allow individuals to check the lawfulness of processing and the right to a copy should not adversely affect the rights of others unreasonably.

To do list

- [ ] Review customer facing teams processes, procedures and training – are they sufficient to deal with the GDPR's access and portability rules?
- [ ] Develop template response letters, to ensure that all elements of supporting information are provided.
- [ ] Assess your organisation's ability to provide data in compliance with the GDPR's format and timing obligations. It may be necessary to develop formatting capabilities to meet access requests.
- [ ] If portability applies, consider which of your records are covered by this. Check if the data (and associated meta data) can easily be exported in structured, machine-readable formats. Look out for industry initiatives to develop interoperable formats.
- [ ] If you provide an IoT/ connected product, or a related service for such a product, or are a gatekeeper, check you can comply with enhanced portability requirements.
- [ ] Consider developing data subject access portals, to allow direct exercise of subject access rights.

Right of information and access

An individual has the following rights with regards to a data controller:

- to obtain confirmation whether their personal data are being processed;
- to access the data (i.e. to a copy not the actual document); and
- to be provided with supplemental information about the processing.

As with all data subject rights, the controller must comply *"without undue delay"* and *"at the latest within one month"*, although there are some possibilities to extend this for a further two months.

Before providing any data to the requester, the controller must also use reasonable means to verify the identity of the person making the request which should be proportionate to the sensitivity of the data being processed– but should not keep or collect data just so as to be able to meet subject access requests. These points are particularly pertinent to online services.

Right of access to data

The controller must provide *"a copy of the personal data undergoing processing"*. This is not a right to the document but rather a copy of the data (Case C-487/21).This case also made a number of other points clear in relation to the right of access to data:

- the controller must give the data subject a faithful and intelligible reproduction of all personal data undergoing processing;
- the right of access must not adversely affect the rights and freedoms of others (which reiterates the necessity for controllers to carry out a balancing exercise between the data subjects' rights and the rights and freedoms of others).

This must be provided free of charge, although the controller may charge a reasonable, administrative-cost fee, if further copies are requested or where the request is manifestly unfounded or excessive which is a high bar to satisfy.

If the request is made in electronic form, the information should be provided in a commonly used electronic form (unless the data subject requests otherwise). This could impose costs on controllers who use special formats, or who hold paper records.

Recital 63 also suggests that, where possible, the controller may provide a secure system which would grant the data subject direct access to their data. This seems to be encouraged rather than required.

Supplemental information

The controller must also provide the following information:

- the purposes of processing;
- the categories of data processed;
- the recipients, or categories of recipients (in particular, details of disclosure to recipients in third countries or to international organisations (bodies governed by public international law or set up by agreement between countries)) – note on request this includes the actual identity of those recipients (CJEU C-154/21) however internal recipients acting under the authority of the controller organization (e.g. employees) are not generally considered 'recipients' for this purpose. Information about other employees who accessed the data subject's personal data would only need to be provided if this was essential to allow the data subject to exercise their rights – and even here the rights and freedoms of those other employees should be taken into account (Case C-579/21);
- the envisaged retention period, or, if this is not possible, the criteria used to determine this period;
- the individual's rights of rectification or erasure, to restrict processing or to object to processing and to lodge a complaint to a supervisory authority;
- information regarding the source of the data (if not collected from the data subject); and
- any regulated automated decision taking (i.e. decisions taken solely on an automated basis and having legal or similarly significant effects; also, automated decision taking involving special categories of data) – including information about the logic involved and the significance and envisaged consequences of the processing for the data subject.

If the controller does not intend to comply with the request or will not provide the response within the deadline, it must also provide reasons.

Exemptions

The GDPR recognises that subject access may adversely affect others and provides that the right to receive a copy of the data shall not adversely affect such rights. Recital 63 notes that this could extend to protection of intellectual property rights and trade secrets (for example, if release of the logic of automated decision taking would involve release of such information). However, the recital also notes that a controller cannot refuse to provide *all* information, on the basis that access may infringe others' rights.

Article 23 GDPR allows under specific conditions, a national or Union legislator to restrict, by way of a legislative measure, the scope of the obligations and rights provided for in the right to access.

Recital 63 also contains two other useful limiting provisions:

- if the controller holds a large quantity of data, it may ask the data subject to specify the information or processing activities to which the request relates. (However, the recital does not go on to say that there is any exemption due to large volumes of relevant data: the limitation seems to be more to do with the specificity of the request, rather than the extent of time and effort on the controller's part – although the two may, of course, be linked);
- the data subject's right is *"to be aware of and verify the lawfulness of the processing"*. This confirms the comments made by the CJEU in *YS v Minister voor Immigratie, Integratie en Asiel* (Case C-141/12) that the purpose of subject access requests is to allow the individual to confirm the accuracy of data and confirm the lawfulness of processing and to allow them to exercise rights of correction or objection if necessary. In other words, the purpose is related to the individual's rights under data protection legislation: requests made for other, non-data protection purposes, may possibly be rejected.

Further reading:

EDPB Guidelines 01/2022 on data subject rights – Right of access

Rectification

Individuals can require a controller to rectify inaccuracies in personal data held about them. In some circumstances, if personal data are incomplete, an individual can require the controller to complete the data, or to record a supplementary statement.

Portability

The subject access right provided under the GDPR already gives individuals the right to require their data to be provided in a commonly used electronic form.

Data portability goes beyond this and requires the controller to provide information in a structured, commonly used and machine-readable form so that it may be transferred by the data subject to another data controller without hindrance.

Further, the controller can be required to transmit the data directly to another controller where it is technically feasible to do so. The GDPR encourages controllers to develop interoperable formats.

Whereas subject access is a broad right, portability is narrower. It applies:

- to personal data which is processed by automated means (no paper records);
- to personal data which the data subject has provided to the controller; and
- only where the basis for processing is consent, or that the data are being processed to fulfil a contract or steps preparatory to a contract.

Data which the individual *"has provided"* is interpreted widely. Pursuant to guidance from the former Article 29 Working Party, this is not limited to forms completed by an individual, but to information gathered by the controller in the course of its dealings with the individual or generated from observation of his or her activity. Examples of occasions when data portability will apply include: (i) data held by a music streaming service, (ii) titles of books held by an online bookstore, (iii) data from a smart meter or other connected objects, (iv) activity logs, (v) history of website usage, (vi) search activities or (vii) emails sent to the individual. However, the portability right does not extend to personal data which is inferred or derived by the data controller (for example, the results of an algorithmic analysis of an individual's behaviour).

Whilst data portability applies only to data controllers, data processors will be under contractual obligations to assist controllers *"by appropriate technical and organisational measures"* with responding to portability requests. Data controllers should therefore implement specific procedures with their processors on handling such requests.

Data portability must not prejudice the rights of others. However, according to supervisory authorities, the original data controller is not responsible for the receiving data controller's compliance. Instead, any organisation receiving the data must ensure that its use of the data is lawful.

There are exemptions from portability - for example, where this would adversely affect IPRs or trade secrets. Supervisory authorities consider that this does not excuse all compliance with the right.

Data portability requirements may also conflict with other access and portability requirements in sector-specific EU (e.g. the right to access one's bank account history under the Payment Services Directive 2) or member state legislation. Guidance from the Article 29 Working Party explains that the GDPR portability right will not apply if the individual makes clear he is exercising his rights under another law. If, however, the individual seeks to exercise his rights under the GDPR, the controller must assess the interplay between any competing rights case-by-case, but the more specific legislation will not automatically displace the GDPR right.

New EU laws

In practice, portability has had limited effect. This is because it only applies to some personal data (provided by the user) and when the lawful basis for processing is consent or contractual necessity - and the controller has one month to comply with requests. The Data Act and the Digital Markets Act create stronger portability rights.

The Data Act applies to manufacturers of connected products where a connected product generates data that is designed to be retrievable by the manufacturer. It also applies to data generated by related services – that is services which allow the user to control the functionality of the connected product (for example, being able to unlock a car remotely). The Data Act provides that product data and related service data must be available to the user without delay and without charge. Where relevant and where technically feasible, there should be real time and continuous access. The user can also require that the data is provided to a third party.

Data which is generated only after additional investment by the manufacturer is excluded and there are protections for trade secrets. If someone other than the data subject to whom the data relates is the end user of the device, then the Data Act takes account of this by providing that data must only be made available to that user when there is a lawful basis for this under GDPR.

Overall, the right granted by the Data Act is stronger than portability under GDPR: it is faster, and, applies to more data (it does not need to be personal; it does not need to be provided by the data subject; and it is not dependent on the lawful basis used by the manufacturer for its processing).

The Digital Markets Act also extends portability. For their regulated services, gatekeepers must ensure effective portability of data provided by the end user or generated through the end-user's activity on the service, again, by continuous and real time access to the data, free of charge.

Where can I find this?

Subject access, Article 15, Recitals 59, 63, 64

Rectification, Article 16

Portability, Article 20 and WP 242, Recital 68

Rights to object

At a glance

- There are rights for individuals to object to specific types of processing:
  - Direct marketing;
  - Processing based on legitimate interests or performance of a task in the public interest/ exercise of official authority; and
  - Processing for research or statistical purposes.
- Only the right to object to direct marketing is absolute (i.e. no need to demonstrate grounds for objecting, no exemptions which allow processing to continue).
- There are obligations to notify individuals of these rights at an early stage - clearly and separately from other information.
- Online services must offer an automated method of objecting.

To do list

- [ ] Audit data protection notices and policies to ensure that individuals are told about their right to object, clearly and separately, at the point of 'first communication'.
- [ ] For online services, ensure there is an automated way for this to be effected.
- [ ] Review marketing suppression lists and processes (including those operated on behalf of your organisation by partners and service providers) to ensure they are capable of operating in compliance with the GDPR.

Rights to object

Three rights to object are given by the GDPR. All relate to processing carried out for specific purposes, or which is justified on a particular basis. There is no right for an individual to object to processing in general.

The rights are to object to:

Processing which is for direct marketing purposes

This is an absolute right; once the individual objects, the data must not be processed for direct marketing any further. This includes profiling to the extent it relates to direct marketing.

Processing for scientific/historical/research/ statistical purpose

Less strong than the right to object to direct marketing – there must be *"grounds relating to [the data subject's] particular situation"*.

There is an exception where the processing is necessary for the performance of a task carried out for reasons of public interest.

Processing based on two specific purposes:

Again, this can be exercised on grounds relating to the data subject's particular situation.

1. legitimate interest grounds (i.e. under Article 6(1)(f)); or

2. because it is necessary for a public interest task/ official authority (i.e. Article 6(1)(e)).

The controller must then cease processing of the personal data unless:

- it can demonstrate compelling legitimate grounds which override the interests of the data subject; or

- the processing is for the establishment, exercise or defence of legal claims.

So, once an individual objects, based on his or her specific situation, the burden falls to the controller to establish why it should, nonetheless, be able to continue processing personal data on this basis.

Article 23 GDPR allows under specific conditions, a national or Union legislator to restrict, by way of a legislative measure, the scope of the obligations and rights provided for in the right to object.

In December 2023 the CJEU issued its judgment in the combined Cases C-26/22 and 64/22 dealing with the retention of insolvency data by Credit Reference Agencies (CRA) in Germany. The Court found that, in circumstances where a CRA sought to retain insolvency data beyond the period during which it was permitted in German law to be published, that retention was unlawful notwithstanding any code of conduct stating the contrary issued by the competent data protection authority. The data subjects had the right to object to the processing of their personal data beyond the statutory period for publication and if the controller could not prove that it had legitimate grounds to continue the processing which overrode the data subjects interests, then the data subject data subject could ask for the data to be erased under Article 17.

Notify individuals of their rights

In the case of processing for direct marketing and processing based on tasks in the public interest/legitimate interests, the individual's right to object must be explicitly brought to his or her attention – at the latest at the time of first communication with the individual. This must be presented clearly and separately from other information.

This need to inform the individual does not apply to statistical/research based processing.

In the case of online services, the individual must be able to exercise his or her right by automated means.

Further reading:

EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR

Where can I find this?

Recitals 69 and 70, Article 21

Right to erasure and right to restriction of processing

At a glance

- More extensive, and unclear rights are introduced: a right to be forgotten (now called erasure) and for processing to be restricted.
- Individuals can require data to be 'erased' when there is a problem with the underlying legality of the processing or where they withdraw consent or when the data subject has objected to the legitimate interests of the controller and there are no overriding grounds to continue processing.
- The individual can require the controller to 'restrict' processing of the data whilst complaints (for example, about accuracy) are resolved, or if the processing is unlawful but the individual objects to erasure.
- Controllers who have made data public or shared data with third parties which is then subject to a right to erasure request, are required to notify others who are processing that data with details of the request. This is a wide-ranging and challenging obligation.
- Where personal data is automatically obtained from third parties which then becomes the subject of an erasure request, controllers must ensure that they request their data providers to not re-provide the personal data that has been erased.

To do list

- [ ] Ensure that members of staff and suppliers who may receive data erasure requests recognise them and know how to deal with them.
- [ ] Determine if systems are able to meet the requirements to mark data as restricted whilst complaints are resolved: undertake development work if needed.

Right to be forgotten

Individuals have the right to have their data 'erased' in certain specified situations - in essence where the processing fails to satisfy the requirements of the GDPR. The right can be exercised against controllers, who must respond without undue delay (and in any event within one month, although this can be extended in difficult cases).

When does the right apply?

- When data are no longer necessary for the purpose for which they were collected or processed.
- If the individual withdraws consent to processing (and if there is no other justification for processing).
  - There is a further trigger relating to withdrawal of consent previously given by a child in relation to online services. However, this seems to add nothing to the general principle that consent can be revoked and, where this is done, that the individual can require the data to be erased.
- To processing based on legitimate interests - if the individual objects and the controller cannot demonstrate that there are overriding legitimate grounds for the processing. The burden of proof will be on the controller and the particular situation of the individual must be taken into account (see section on rights to object above).
- When the data are otherwise unlawfully processed (i.e. in some way which is otherwise in breach of the GDPR).
- If the data have to be erased to comply with Union or Member State law which applies to the controller.

The last condition could, for example, apply if an individual considers that a controller is retaining personal data where legislation stipulates that such data (for example an employment related check) must be deleted after a specified period of time.

The general catch-all allowing erasure requests to be made where data are *'unlawfully'* processed is potentially onerous: there are many reasons why data could be processed unlawfully under the GDPR (they may be inaccurate; an element of an information notice may not have been provided to the individual). However, it is not obvious that this should grant a right for the data to be erased. It will be therefore important to consider how Member States apply the exemption provisions.

Data put into the public domain

If the controller has made personal data public, and where it is obliged to erase the data, the controller must also inform other controllers who are processing the data that the data subject has requested erasure of those data. The obligation is intended to strengthen individual's rights in an online environment.

The obligation is to take *reasonable steps* and account must be taken of available technology and the cost of implementation. However, the obligation is potentially wide-reaching and extremely difficult to implement: for example, as this is now public domain data, one question is how the original controller will be able to identify the controllers it needs to notify.

Other obligations to notify recipients

If the controller has to erase personal data, then the controller must notify anyone to whom it has disclosed such data, unless this would be impossible or involve disproportionate effort.

Exemptions

The obligation does not apply if processing is necessary:

- for the exercise of the right of freedom of expression and information;
- for compliance with a Union or Member State legal obligation;
- for performance of a public interest task or exercise of official authority;
- for public health reasons;
- for archival, research or statistical purposes (if any relevant conditions for this type of processing are met); or
- if required for the establishment, exercise or defence of legal claims.

See section on derogations and special conditions for other occasions when exemptions may be relevant - if provided for under Union or Member State law.

Further reading:

EDPB Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)

Where can I find this?

Right to erasure, Article 17 and 21, Recitals 38, 65 and 66 EDPB 5/2019

Right to restriction of processing

This replaces the provisions in the former Data Protection Directive on 'blocking'. In some situations, this right gives an individual an alternative to requiring data to be erased; in others, it allows the individual to require data to be held in limbo whilst other challenges are resolved.

What is restriction?

If personal data are 'restricted', then the controller may only store the data. It may not further process the data unless:

- the individual consents; or
- the processing is necessary for the establishment, exercise or defence of legal claims; for the protection of the rights of another natural or legal person; or for reasons of important (Union or Member State) public interest.

Where the data are processed automatically, then the restriction should be effected by technical means and noted in the controller's IT systems. This could mean moving the data to a separate system; temporarily blocking the data on a website or otherwise making the data unavailable.

If the data have been disclosed to others, then the controller must notify those recipients about the restricted processing (unless this is impossible or involves disproportionate effort).

The controller must notify the individual before lifting a restriction.

When is restriction applicable?

- When an individual disputes data accuracy, then personal data will be restricted for the period during which this is verified;
- When an individual has objected to processing (based on legitimate interests), then the individual can require the data to be restricted whilst the controller verifies the grounds for processing;
- When the processing is unlawful but the individual objects to erasure and requests restriction instead; and
- When the controller has no further need for the data but the individual requires the personal data to establish, exercise, or defend legal claims.

The last condition, for example, means that controllers are obliged to retain data storage solutions for former customers if the personal data are relevant to proceedings in which the individual is involved.

Commentary in case law on the right to erasure or restriction of processing

Case C-60/22 considered a situation where the controller had failed to conclude an arrangement determining joint responsibility for processing (Article26) and to maintain a record of processing activities (Article30)) and where a data subject sought to assert that this triggered the right to erasure. The CJEU determined that this does not constitute unlawful processing conferring a right on the data subject of erasure or restriction of processing, where this failure does not amount to infringement of the principle of *"accountability"* set out in Article 5(2) GDPR.

Where can I find this?

Right to erasure, Article 17 and 19, Recitals 65, 66, 73

Right to restriction, Article 18 and 19, Recitals 67 and 73

Profiling and automated decision-taking

At a glance

- The automated decision-taking rules affect decisions:
  - taken solely on the basis of automated processing; and
  - which produce legal effects or have similarly significant effects.
- Where the decision is:
  - necessary for the entry into or performance of a contract; or
  - authorised by Union or Member State law applicable to the controller; or
  - relies on or uses individual's explicit consent

  then automated processing can be used. However, suitable measures to protect the individual's interests must still be in place.
- There are additional restrictions on profiling based on special category data – which need explicit consent, or to be authorised by Union or Member State law which is necessary on substantial public interest grounds.

To do list

- [ ] Check what significant automated decision-taking is used. Identify any decisions which rely on:
  - Consent;
  - Authorisation by law; or
  - Data which relates to special category data or children.
- [ ] If automated decision-taking is based on consent, ensure this is explicit.
- [ ] If automated decision-taking relies on or uses special categories of data:
  - Check if you can obtain explicit consent;
  - If not, you can only carry out such processing where authorised by Union or Member State law.
- [ ] If automated decision-taking involves children, seek advice: this is restricted.

Meaning of profiling

Profiling is *"any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement"*.

During the original legislative process, there were attempts to introduce significant restrictions on all profiling. However, in the end, these were not included – although Recital 72 does note that the EDPB may publish guidance on profiling. In May 2018, the EDPB endorsed the former Article 29 Working Party's Guidelines on Automated Decision Making and Profiling (WP 251 rev.01).

Restrictions on automated decision-taking with significant effects

Restrictions on decisions based solely on automated processing (which could include profiling), apply if the decisions produce legal effects or similarly significantly affects the data subject. Recital 71 gives the examples of online credit decisions and e-recruiting; it also makes clear that the objectionable element is the lack of meaningful human intervention.

According to the EDPB Guidelines, *"legal effects"* are those that have an impact on an individual's legal rights such as statutory or contractual rights (for example an individual being refused entry at a border, being denied a social benefit granted at law or cancellation of a contract). *"Similarly significant effects"* are those that are equivalent or similarly significant to legal effects. The effect must be more than trivial and must have the potential to significantly influence the circumstances, behaviour or choices of the individuals concerned (examples could include automatic refusal of an online credit application or e-recruiting practices without meaningful human intervention). Much depends on the context, and it is difficult to provide a fixed list of what might be considered 'significant'.

In the *Schufa* case (CJEU C-634/21), the CJEU held that credit reference agencies are undertaking automated individual decision making when they create a probability based credit score and where third parties, such as lenders, rely heavily on this when evaluating loan applications.

The CJEU rejected arguments that the lenders were taking the decisions and that the credit reference agencies were engaging in preparatory acts.

Such significant automated processing can be used if it is:

- necessary to enter into, or to perform, a contract between a data subject and a controller;
- authorised by Union or Member State law; or
- based on the individual's explicit consent.

Recital 71 also notes that such measures should not concern children.

Automated decisions based on explicit consent or contractual fulfilment

In the first and third cases (contract performance and consent), the controller must implement suitable measures to safeguard the data subject. At a minimum, this must include a right to obtain human intervention for the data subject to be able to express his or her point of view and to contest the decision.

The equivalent provisions in the former Data Protection Directive stated that this was not necessary if the effect of the decision was to grant the individual's request. This was not carried across into the GDPR.

Recital 71 emphasises that appropriate statistical techniques must be used; that transparency must be ensured; that measures should be in place to correct inaccuracies and risks of errors; and that security must be ensured and discriminatory effects prevented.

According to the above Guidelines, controllers should carry out regular testing on the data sets they process to check for any bias and measures should be taken to prevent errors, inaccuracies or discrimination on the basis of special categories of data. Audits of algorithms are also advised.

Authorisation by law

In the second case (authorisation by law) the law itself must contain suitable measures to safeguard the individual's interests. Recital 71 mentions profiling to ensure security and reliability of services or in connection with monitoring of fraud and tax evasion as types of automated decisions which could be justified based on Union or Member State law.

Special category data

Automated decision-taking based on special category data is further restricted. Decisions based on these types of data may only take place:

- with explicit consent; or
- where the processing is necessary for substantial public interest reasons and on the basis of Union or Member State law – which must include measures to protect the interests of the data subjects.

New EU Laws

Under the Digital Services Act, extra provisions on profiling are outlined for online platforms that, at the request of the recipient of the service, store and disseminate information to the public. Specifically, these platforms are prohibited from (i) using special categories of data (e.g., racial, or ethnic origin, political beliefs, and health data) for profiling for advertising (Article 26(3) DSA), and (ii) using profiling for advertising when it is known that the user is a minor (Article 28(2) DSA).

The Digital Markets Act also contains provisions on profiling. Gatekeepers are required to publish information on their use of profiling and to undergo an independent audit of their profiling. The results of the audit must be shared with the Commission which, in turn, will share this with EDPB (Article 15 DMA).

Further reading:

Former Former Article 29 Guidelines on Automated Decision Making and Profiling (WP 251 rev.01) (endorsed by EDPB).

EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR

Judgment of the Court (First Chamber) of 7 December 2023. OQ v Land Hessen (SCHUFA Case C-634/21.

Case C-203/22 Dun & Bradstreet Austria

Where can I find this?

Article 4(4) & 22, Recitals 71 & 72

Data governance obligations

At a glance

- The GDPR requires all organisations to implement a wide range of measures to reduce the risk of their breaching the GDPR and to prove that they take data governance seriously.
- These include accountability measures such as: DPIAs, audits, policies, records of processing activity and (potentially) appointing a Data Protection Officer (*"DPO"*).

To do list

- [ ] Assign responsibility and budget for data protection compliance within your organisation. Whether or not you decide to appoint a DPO (or have to), the GDPR's long list of data governance measures necessitates ownership for their adoption being allocated.
- [ ] Ensure that a full compliance programme is designed for your organisation, incorporating features such as: DPIAs, regular audits, policy reviews and training and awareness raising programmes.
- [ ] Audit existing supplier arrangements and ensure template RFP and procurement contracts reflect the GDPR's data processor obligations.
- [ ] Monitor the release of supervisory authorities / EU and industry published supplier terms and codes of practice to see if they are suitable for use by your organisation.
- [ ] Refine and keep up to date records of your organisation's processing activities.

The GDPR enshrines a number of *"data governance"* concepts, the virtues of which law makers and supervisory authorities have extolled for some time. These concepts create significant operational obligations and costs for many public and private sector organisations.

A general obligation is imposed upon controllers to adopt appropriate technical and organisational measures to meet their GDPR obligations (and to be able to demonstrate that they have done so).

Data Protection by Design & Default (aka "Privacy by design")

Controllers are required to put in place appropriate technical and organisational measures which:

- are designed to implement data protection principles and to integrate safeguards for the protection of data subjects' rights; and
- ensure that, by default, only personal data that are needed for the specific purpose of the processing are used.

When considering the design of technical and organisational measures, the GDPR directs controllers to assess the state of the art, cost of implementation, and the nature, scope and reasons for use, together with the different levels of risks posed to individuals' rights and freedoms by the given use of personal data. The GDPR states that such an assessment should be undertaken both when deciding how to process personal data and whilst processing personal data. Example measures to meet the data minimisation principle referenced in the GDPR include adopting appropriate staff policies and using pseudonymisation.

Further information about what organisations are expected to do may be the found in the EDPB's Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (the *"DPbyDD Guidelines"*), which were adopted on 20 October 2020. The DPbyDD Guidelines focus on the interpretation of the requirements in Article 25 GDPR, exploring the legal obligations imposed and providing a number of operational examples. Other topics covered by the DPbyDD Guidelines include certification mechanisms for compliance with Article 25, how Article 25 may be enforced by supervisory authorities, and recommendations for stakeholders (which includes processors and technology providers) on how the EDPB considers that data protection by design and default may be successfully implemented.

Joint controller arrangements

Joint controllers (that is, two or more controllers who jointly determine the purpose and means of processing) are required to arrange between themselves their respective responsibilities for compliance with the GDPR – and, in particular, the exercise of data subjects' rights and provision of transparency information to individuals. The arrangement must set out the parties' roles and responsibilities with respect to data subjects, and the essence of the arrangement must be made available to data subjects (e.g. by way of a privacy notice).

Whilst there is no legislative requirement for an arrangement between joint controllers to be set out in a formal contract, it would be sensible to do so e.g. for accountability reasons. The EDPB in its Guidelines 07/2020 on the concepts of controller and processor in the GDPR (*"Concepts of C&P Guidelines"*) adopted on 7 July 2021, confirm that documentation of "*the relevant factors and internal analysis carried out in order to allocate the different obligations*" is recommended. The Concepts of C&P Guidelines focus on the assessment around how a determination of joint controllership may be found and

the requirements on the parties when joint controllership is determined.

Since the coming into effect of the GDPR, the CJEU has issued a number of judgments which explored the concept of joint controllership, albeit under the provisions of the Data Protection Directive. A key takeaway from this case law is that quite a broad interpretation of joint controllership is emerging.

Key cases include:

- the *"Facebook Fan Page"* case (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH (Case C-210/16));
- the *"Jehovah's Witness"* case (referenced by Tietosuojavaltuutettu (Case C-25/17)); and
- The *"Facebook 'Like Button'"* case (Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (Case C-40/17)).

Data Protection Impact Assessments (DPIAs)

What is a DPIA and when is it required?

A Data Protection Impact Assessment, also known as a Privacy Impact Assessment, is a process for demonstrating compliance and assessing and mitigating risk. The GDPR formalises a requirement for DPIAs to be carried out in certain circumstances. Specifically, controllers must ensure that a DPIA has been completed with respect to any *"high risk"* processing activity before it is commenced. *"High risk"* here is measured by reference to the risk of infringing a natural person's rights and freedoms.

Examples of high risk processing set out in the GDPR include:

- systematic and extensive processing activities, including profiling and where decisions have legal effects - or similarly significant effects - on individuals;
- large scale processing of special categories of data or criminal convictions or offence details; or
- large scale, systematic monitoring of public areas (e.g. CCTV).

Guidelines (WP248 rev.01) issued in 2017 and endorsed by the EDPB (the *"DPIA Guidelines"*), indicate that other factors may increase risk, including the presence of vulnerable data subjects (e.g. children and, notably, employees), matching or combining data sets in unexpected ways from the perspective of the affected individuals, and processing designed to deny an individual a right or access to a contract or service.

Organisations should take care to also check local requirements. Most EU countries have issued and had approved by the EDPB their lists of personal data processing activities which require a DPIA or (as is the case for a handful) do not under Articles 35(4) and (5).

Is there a set form for DPIAs?

There is no mandated form for a DPIA and, as noted by the DPIA Guidelines, numerous templates already exist.

Interestingly, the DPIA Guidelines took account of two relevant ISO documents - one on risk management and one on DPIAs in an information security context.

As a minimum, the GDPR requires that a DPIA include:

- A description of the envisaged processing operations and the purposes of the processing;
- An assessment of (i) the need for and proportionality of the processing and (ii) the risks to data subjects (as viewed from the perspective of data subjects) arising; and
- A list of the measures envisaged to (i) mitigate those risks (including non-data protection risks, such as infringements on freedom of thought and movement) and (ii) ensure compliance with the GDPR.

What else are we required to do?

If a DPO has been appointed (see below), their advice on the carrying out of a DPIA must be sought.

Consulting the supervisory authority is required prior to any processing of personal data whenever risks cannot be mitigated and remain high - such as where individuals may encounter significant or even irreversible consequences as a result of the processing. The GDPR contains specific procedural directions for this process.

Controllers are directed to seek the views of affected data subjects *"or their representatives"* in conducting a DPIA, if appropriate. In the context of HR data processing this has been interpreted as an obligation to consult with employees, or their representatives, such as works councils or Trade Unions.

Data Protection Officer (DPO)

Controllers and processors are free to voluntarily appoint a DPO, but the following are obligated to do so:

- Public authorities (with some minor exceptions);
- Any organisation whose core activities require:
  - *"regular and systematic monitoring"* of data subjects *"on a large scale"*; or
  - *"large scale"* processing of special categories of data or criminal convictions and offences data; and
- Those obliged to do so by local law (countries such as Germany are likely to fall into this category).

The DPO Guidelines (WP 243) can help organisations interpret the terms *"core activities", "regular and systematic monitoring"* and *"large scale"*. These guidelines include the following points:

- *"Core activities":* Activities which are *'an inextricable part'* of the controller's / processor's pursuit of its goals are cited. Reassuringly the DPO Guidelines confirm that an organisation's processing of its staff information (which is highly likely to include special categories of data) is ancillary to its activities, not core. Examples of core activities given include: a security company's surveillance where it is hired to safeguard a public space; a hospital's processing of patient health data and an outsourced provider of occupational health services' processing of its customer's employee data.
- *"Regular and systematic monitoring":* All forms of online tracking and profiling are called out as examples by the EDPB, including for the purpose of behavioural advertising and email retargeting. Other examples cited include: profiling and scoring (e.g. for credit scoring, fraud prevention or for the setting of insurance premiums); location tracking; fitness and health data tracking; CCTV; processing by connected devices (smart meters, smart cars etc); and data-driven marketing activities (i.e. big data).
- *"Large scale"*: here, the EDPB says that it is not currently keen on precise numbers being used as a benchmark for this term, but that plans are afoot to publish thresholds in the future. Instead, the DPO Guidelines (last revised in April 2017) list some fairly obvious generic factors to be considered in defining large scale (e.g. the number of individuals affected and geographic extent of processing). Examples of large scale processing cited include: a bank or insurance company processing customer data; and processing of an international fast food chain's customer geo-location data in real time for statistical purposes by a specialist processor.

The DPO Guidelines confirm that where a DPO is appointed on a voluntary basis, the same requirements as set by the GDPR to mandatory DPOs will apply to them. Moreover, once an organisation opts to appoint a DPO, it cannot circumscribe the scope of the DPO's review – the DPO must have the authority to review all data processing.

In response to an uncertainty in the GDPR, the DPO Guidelines confirm that nothing prevents an organisation from assigning the DPO with the task of maintaining the records of processing operations.

Interestingly, the DPO Guidelines also recommend that an organisation which decides not to voluntarily appoint a DPO documents why it thinks that it is not subject to the DPO appointment criteria (as summarised above). Such assessments should be kept up to date

and revisited when new activities or services are contemplated.

If a DPO is not mandatory and a DPO is not appointed voluntarily, staff or consultants can be appointed to carry out similar tasks, but the EDPB says that to avoid confusion they should not be called DPOs.

Where appointed, a DPO must be selected by reference to their professional qualities and expert knowledge (which employers are obliged to help maintain). Critically, while they may be supported by a team, there can only be one DPO per organisation and that person should preferably be located in the EU. The DPO Guidelines note that the more sensitive or complex an organisation's data processing activities are, the higher the level of expertise that its DPO will be expected to have.

Organisations must ensure that their DPO's primary objective is ensuring compliance with the GDPR. Their tasks should at a minimum include: advising their colleagues and monitoring their organisation's GDPR/ privacy law/policy compliance, including via training and awareness raising, running audits, advising regarding DPIAs and cooperating with supervisory authorities. The DPO Guidelines stress that DPOs will not be personally liable for their organisation's failure to comply with the GDPR. Liability will fall upon the organisation, including if it obstructs or fails to support the DPO in meeting their primary objective.

Adequate resources must be provided to enable DPOs to meet their GDPR obligations, and they should report to the highest level of management.

Group companies can appoint a single DPO. A DPO can be a member of staff or a hired contractor. Key features of a DPO's skillset (according to the DPO Guidelines) include that they must be knowledgeable about the organisations they represent and accessible - including that they are able to easily communicate with supervisory authorities and data subjects (e.g. customers and staff) in countries in which the organisation operates. It seems that the DPO Guidelines therefore expect DPOs to be polyglots as well as data protection experts - or at least to have easy access to good translation facilities.

Controllers and processors must ensure that their DPO is involved in all material matters regarding data protection (including, according to the DPO Guidelines on the topic, following a personal data breach), and can operate independently of instruction and will not be dismissed or penalised for performing their task. It remains to be seen how employment laws will interpret this provision. Organisations must ensure there is a secure and confidential channel by which employees can communicate with the DPO.

The DPO Guidelines also state that if an organisation's management do not agree with and decides not to follow a DPO's recommendation then they should formally record this and the reasons for their decision. The DPO Guidelines also warn that instruction must not be given to the DPO regarding how to deal with a matter, what results should be achieved or whether or not to consult with a regulatory authority.

The GDPR does not restrict DPOs from holding other posts but expressly requires that organisations ensure that such other tasks do not give rise to a conflict of interest for the DPO. The DPO Guidelines go further by saying that a DPO cannot hold senior positions in management (i.e. as a CEO, COO or CFO). Other senior managers, including Head of HR, Marketing or IT, or lower level employees who make decisions about the purposes and means of processing are also barred from the position. If an external DPO (e.g. a lawyer) provides day-to-day DPO services to controllers or processors, this may prevent this individual from representing those entities before courts in cases involving data protection issues.

The DPO's contact details must be published and also notified to an organisation's supervisory authority as the DPO is to be a point of contact for questions about data protection compliance matters.

Bird & Bird assists organisations with this obligation and can be appointed as GDPR DPO. Contact Bird & Bird Privacy Solutions if you would like further details about our DPO services.

"GDPR" Representatives

Many non-EU *"established"* organisations which target or monitor EU data subjects are required by the GDPR to designate in writing a representative which is located in the EU. This *"GDPR Representative"* must be mandated by an organisation as an alternative or additional port of call to which data subjects and supervisory authorities may turn for all issues relating to the processing which is in scope of the GDPR.

A GDPR Representative need not be appointed by a public authority, or an organisation which carries out occasional, non-large scale, processing of special categories of data or criminal convictions and offences data which is *"unlikely to result in a risk to the rights and freedoms of natural persons"*. EDPB guidance on the territorial scope of the GDPR states that *"public body"* should be interpreted in accordance with national law, and that further guidance relating to *"large scale"* and *"occasional"* processing may be found in its DPO Guidance and position paper on Article 30 GDPR, respectively.

Bird & Bird now assists non-EU established organisations with this obligation and can be appointed as GDPR representative.

Do not hesitate to contact Bird & Bird Privacy Solutions if you would like further details about our GDPR representative services.

Using service providers (data processors)

Article 28 GDPR imposes a high duty of care upon controllers in selecting their personal data processing service providers which will require procurement processes and request for tender documents to be regularly assessed.

Contracts must be implemented with service providers which include a range of information (e.g. the data processed and the duration for processing) and obligations (e.g. assistance where a personal data breach occurs, appropriate technical and organisational measures taken and audit assistance obligations, to name but a few). These obligations must also be flowed down where a service provider engages a sub-processor.

On the 4 June 2021, the European Commission published a set of standard contractual clauses between controllers and processors (*"Article 28 Clauses"*) to cover the requirements set out under Article 28 of the GDPR. These are not mandatory clauses and are instead intended to provide an option for organisations to use as an annex to commercial agreements in order to comply with the Article 28 requirements. The Article 28 Clauses should not be confused with the standard contractual clauses discussed below in relation to international data transfers.

Record of processing activities

Organisations are obliged to keep a record of their processing activities (the type of data processed, the purposes for which it is used etc).

Data processors are also required to maintain such a record about personal data which controllers engage them to process, a requirement which is particularly challenging for many cloud and communications service providers.

Whilst an exemption from the above obligations applies to organisations employing fewer than 250 people, this exemption does not apply where data relating to criminal convictions and offences are processed, as well as where special categories of data are processed, which seems likely to nullify its usefulness, particularly in the employment context.

Where can I find this?

Privacy by Design, Article 25, Recitals 74-78

PIAs, Articles 35-36, Recitals 89-94

DPOs, Articles 37-39, Recital 97, WP 243

Using data processors, Articles 28 and 29, Recital 81

Record of processing activities, Article 30, Recital 82

Personal data breaches and notification

At a glance

- Data controllers and data processors are subject to a general personal data breach notification regime.
- Data processors must report personal data breaches to data controllers.
- Data controllers must report personal data breaches to the relevant supervisory authority and in some cases, affected data subjects, in each case following specific GDPR provisions.
- Data controllers must maintain an internal breach register.
- Non-compliance can lead to an administrative fine up to €10,000,000 or in case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- As things stand, the specific breach notification regime for communications service providers, set out in Commission Regulation 611/2013 on the measures applicable to the notification of personal data breaches under the e-Privacy Directive 2002/58/EC, still applies (and forms part of retained law in the UK).

To do list

- [ ] In line with the accountability principle laid down by the GDPR, data controllers and data processors should ensure they have in place internal breach notification procedures, including incident identification systems and incident response plans.
- [ ] Such procedures should be regularly tested and re-reviewed.
- [ ] Work with your IT/IS teams to make sure they implement appropriate technical and organisational measures to render the data unintelligible in case of unauthorised access.
- [ ] Insurance policies should be kept under review to assess the extent of their coverage in case of breaches.
- [ ] Template MSA/data protection clauses and tender documentation should: (i) require suppliers to proactively notify breaches to them; and (ii) put a great emphasis on the duty to cooperate between the parties.

Incidents which trigger notification

The GDPR defines a personal data breach as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"*. On 28 March 2023, the EDPB also adopted Guidelines 9/2022 on personal data notification under the GDPR which provided further guidance on notifications (*"Breach Notification Guidelines"*). The breach notification regime under the GDPR applies as follows:

1. Obligation for data processors to notify data controllers

Timing:

Without undue delay after becoming aware of it.

Exemption:

None.

Observations:

- All breaches have to be reported by the processor to the controller. Where there are multiple controllers affected by the processor's breach, the processor must notify each affected controller.
- The Breach Notification Guidelines recommend that the contract between the controller and processor set out timing, which can include requirements for early notification by the processor.
- The EDPB recommends phased notification in order to help the controller meet the requirement of notifying the supervisory authority within 72 hours.
- The EDPB also acknowledges that, whilst the legal responsibility to notify remains with the controller, a processor could make a notification on the controller's behalf where the controller has authorised the processor to do so as part of the contractual arragements between the parties.

2. Obligation for data controllers to notify the supervisory authority

Timing:

Without undue delay and, where feasible, not later than 72 hours after becoming aware of it.

Exemption:

No reporting if the breach is unlikely to result in a risk to the rights and freedoms of natural persons (e.g. the personal data are already publicly available and a disclosure of such data does not constitute a likely risk to the individual).

Observations:

- In the Breach Notification Guidelines, the EDPB recognises that the precise moment a controller becomes aware of a breach will depend on the circumstances of the specific breach. However, the guidelines state that a controller should be regarded as having becoming *"aware"* when the controller has a reasonable degree of certainty that an incident has occurred that has led to the personal data being compromised. The EDPB goes further in stating that the controller's technical and organisational measures should allow the controller to establish immediately whether a breach has taken place.
- In the EDPB's view, the 72-hour period should be used by the controller to assess the likely risk to individuals in order to determine whether the requirement for notification has been triggered, as well as the action(s) to address the breach, including escalations to the appropriate level of management. Such assessments may be influenced by DPIAs previously conducted by the controller.
- The GDPR provides the possibility for phased notification in the event the controller is unable to provide all the required information to the supervisory authority. However, when the timing obligation is not met, reasons will have to be provided to the supervisory authority (e.g. request from a law enforcement authority or multiple data breaches over a short period of time).
- In the Breach Notification Guidelines, the EDPB recognises the possibility of a controller submitting a *"bundled"* notification where the

same event results in similar but multiple breaches. However, where a series of breaches concern different types of personal data, breached in different ways, then each breach must be reported separately.

3. Obligation for data controller to communicate a personal data breach to data subjects

The data controller must communicate a personal data breach to data subjects only where the breach is likely to result in a high risk to the rights and freedoms of natural persons.

If the data controller is yet to do so, the supervisory authority may compel the data controller to communicate a personal data breach with affected data subjects unless one of the exemptions is satisfied.

Timing:

Without undue delay: the need to mitigate an immediate risk of damage would call for a prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify more time for communication. The EDPB recognises that in exceptional circumstances, communication with data subjects may precede notification to the supervisory authority; for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

No reporting if:

- the breach is unlikely to result in a high risk for the rights and freedoms of data subjects;
- appropriate technical and organisational protection were in place at the time of the incident that rendered the personal data unintelligible (e.g. encrypted data, where the encryption key is still intact and the compromised data is still overwise available);
- immediately following the personal data breach, the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise; or
- this would trigger disproportionate efforts (instead a public information campaign or *"similar measures"* should be relied on so that affected individuals can be effectively informed).

Cross-border personal data breaches

Where a personal data breach affects data subjects in more than one Member State, then the data controller should notify, if it has a single or main establishment, its competent lead supervisory authority (see section on cooperation and consistency between supervisory authorities). This may not necessarily be where the affected data subjects are located or where the breach has taken place. When notifying the lead authority, the data controller should indicate whether the breach affects data subjects in other Member States.

Where an organisation established outside of the EU is subject to the GDPR and experiences a personal data breach, the EDPB recommends that notification should be made to each supervisory authority for which affected data subjects reside in their Member State. The Breach Notification Guidelines state that the mere presence of a representative in a Member State does not trigger the one-stop-shop mechanism.

Documentation requirements

Internal breach register: obligation for the data controller to document each incident *"comprising the facts relating to the personal data breach, its effects and the remedial action taken"*. It is also advisable to have an internal personal data breach response plan that clearly sets out how such breaches and subsequent notifications are dealt with. The supervisory authority can be requested to assess how data controllers comply with their data breach notification obligations.

There are also prescribed requirements to satisfy in the communication to the supervisory authority (e.g. describing the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned, etc.) and the communication to affected individuals (e.g. describe in clear and plain language the nature of the personal data breach and provide at least the following information: (i) the name and contact details of the DPO or other contact point where more information can be obtained; (ii) the likely consequences of the personal data breach; and (iii) the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, to mitigate its possible adverse effects). Many supervisory authorities have produced standard forms for notification of personal data breaches.

Sanctions in case of non-compliance

Failure to meet the above requirements exposes the organisation to an administrative fine of up to €10,000,000 or in case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

In addition, certain Member States are adding at country level criminal liability sanctions in case of non compliance (e.g. France).

What about other EU breach notification regimes?

As things stand, Regulation 611/2013 – which details a specific procedure for breach notification (laid out in Directive 2002/58/EC (the *"e-Privacy Directive"*) as amended) - still applies to providers of publicly available telecommunications services (e.g. telecommunication companies, ISPs and email providers).

At the time of writing, and seven years on from when the European Commission published its proposed text for the new e-Privacy Regulation on 10 January 2017, a final draft of the e-Privacy Regulation has yet to be approved by the European law makers.

For the UK, the substantive requirements of Regulation 611/2013 are retained in UK law notwithstanding the UK's exit from the EU – albeit with appropriate adjustments, (e.g. to replace references to the competent supervisory authority with references to the ICO or relevant Secretary of State) (Electronic Communications (Amendment etc). (EU Exit) Regulations 2019/919.

In addition, the breach notification requirements under cybersecurity laws, including in particular the new Directive (EU) 2022/2555 (the *"NIS2 Directive"*), will need to be considered. The NIS2 Directive will replace the NIS Directive from 18 October 2024, amending the rules on the security of network and information systems in 18 sectors (see our NIS2 Directive Implementation Tracker). Once implemented locally by EU Member States, the new enhanced cybersecurity and reporting requirements will apply to a wide range of companies (including, cloud computing service providers, data centres and online marketplaces) that meet certain company size thresholds and provide their services or carry out their activities within the EU.

If the NIS2 Directive, in conjunction with its local implementation, applies to an organisation, depending on the circumstances of an incident, that organisation would also need to notify the cybersecurity authorities and the recipients of its services. In practice, this means that, in preparation for such incident reporting, organisations within the scope of this major piece of cybersecurity legislation will need to:

- review current processes and procedures to assess what changes need to be made to align with the NIS2 requirements; and

- update incident response plans and processes, including those aimed at complying with the GDPR and other legislation.

Where can I find this?

Recitals 85-88, Articles 33, 34, 70, 83 & 84

Codes of conduct and certifications

At a glance

The GDPR makes provision for the approval of codes of conduct (*"Codes"*) and the accreditation of certifications, seals and marks to help controllers and processors demonstrate compliance and best practice.

Codes of conduct:

- Associations and representative bodies may prepare Codes for approval, registration and publication by a supervisory authority, or, where processing activities take place across member states, by the EDPB. The European Commission may declare Codes recommended by EDPB to have general validity within the EU.
- Codes may be approved in relation to a wide range of topics and adherence to Codes will help controllers and processors demonstrate compliance with GDPR obligations.
- Compliance with Codes will be subject to monitoring, which may be carried out by suitably qualified, accredited bodies. Controllers and processors who are found to have infringed a relevant Code may be suspended from participation in the Code and reported to the supervisory authority.

Certifications, seals and marks:

- The establishment of data protection certification mechanisms and of seals and marks is to be encouraged.
- Certificates will be issued by accredited certifying bodies.
- Certification is voluntary but certification will enable controllers and processors to demonstrate compliance with the GDPR.
- Certificates will be valid for three years and subject to renewal.
- EDPB will maintain a publicly available register of all certification mechanisms, seals and marks.

To do list

- [ ] Organisations should follow developments and consider whether they will wish to apply for certification or comply with a Code that has been approved and published by the EDPB.
- [ ] Once certification schemes are established, controllers should familiarise themselves with relevant schemes and take account of certifications, seals and marks when selecting their processors/ service providers.

Codes of conduct

Although not yet providing a significant aspect of the data protection regime in the EU, when momentum grows in relation to Codes, it is expected that they will become an important component in broadening and adapting the tools for data protection compliance that controllers and processors can draw on, by way of a *"semi-self-regulating"* mechanism.

It is expected that Codes will provide authoritative guidance on certain key areas including:

- legitimate interest in specific contexts;
- pseudonymisation;
- exercise of data subjects' rights;
- protection of minors and modes of parental consent;
- proper implementation of privacy by design and by default, and security measures;
- personal data breach notification; and
- dispute resolution between controllers and data subjects.

The development and the approval of Codes are likely to deliver a number of benefits including:

- establishing and updating best practice for compliance in specific processing contexts;
- enabling data controllers and processors to commit to compliance with recognised standards and practices and be recognised for doing so;
- adherence to Codes can demonstrate that data importers (controllers as well as processors) located outside the EU / EEA have implemented adequate safeguards in order to permit transfers under Article 46; transfers made on the basis of an approved Code together with binding and enforceable commitments of the importer to apply appropriate safeguards may take place without any specific authorisation from a supervisory authority and Codes may therefore offer an alternative mechanism for managing international transfers, standing on the same level as standard contractual clauses and BCR.

Approval of Codes

Codes proposed by associations or representative bodies in relation to data processing activities that affect only one Member State are to be submitted to the competent supervisory authority, for comment and – subject to possible modifications or extensions – approval. Some supervisory authorities are taking steps towards implementing such Codes, for example the French supervisory authority (the CNIL) has approved a Code relating to cloud infrastructure providers and has indicated that other sector- specific Codes such as for medical research are being prepared.

If a Code covers processing operations in several Member States, it should be submitted to the EDPB for an opinion. Subject to possible modifications or extensions, the Code and the EDPB opinion may then be submitted to the European Commission which, upon due examination, may declare its general validity. Codes are to be kept and made available in publicly accessible registers.

Monitoring of compliance

Monitoring of compliance with Codes will be carried out only by bodies accredited by the competent supervisory authority.

In order to become accredited such bodies will have to demonstrate:

- their independence and expertise;
- that they have established procedures to assess the ability of controllers and processors to apply the Code, and to monitor compliance, as well as periodically review the Code;
- the ability to deal with complaints about infringements; and
- that they have processes in place to avoid conflicts of interest.

Accreditations are revocable if the conditions for the accreditation are no longer met.

In June 2019, the EDPB adopted guidelines on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 (the *"Code of Conduct Guidelines"*). The Code of Conduct Guidelines set out the criteria against which Codes will be assessed and how they will be approved.

Certifications, seals and marks

The concept of certifying data processing operations is a significant development in creating a reliable and auditable framework for data processing operations. It is likely to be particularly relevant in the context of cloud computing and other forms of multi-tenancy services, where individual audits are often not feasible in practice.

Member States, supervisory authorities, the EDPB and the Commission are all encouraged to establish data protection certification mechanisms, seals and marks, with regard to specified processing operations.

The competent supervisory authority or the EDPB will approve criteria for the certifications. The EDPB may develop criteria for a common certification, the European Data Protection Seal.

In 2018, the EDPB published guidelines on certification and identifying certification criteria in accordance with Articles 42 and 43 of the GDPR.

There are two key advantages of certificates:

- controllers and processors will be able to demonstrate compliance, in particular with regard to implementing technical and organisational measures.
- certificates can demonstrate that data importers (controllers as well as processors) located outside the EU / EEA have implemented adequate safeguards for the purpose of Article 46; transfers made on the basis of an approved certification mechanism together with binding and enforceable commitments of the importer to apply appropriate safeguards may take place without any specific authorisation from a supervisory authority and certificates therefore offer an alternative mechanism for managing international transfers, standing on the same level as standard contractual clauses and BCR.

Certificates on processing operations will be issued for a period of three years, and are subject to renewal or withdrawal where the conditions for issuing the certificate are no longer met.

The EDPB is to maintain a publicly available register with all certification mechanisms, data protections seals and marks. Certificates can be issued by – private or public – accredited certification bodies. National Accreditation Bodies and/or supervisory authorities may accredit certification bodies (so that they can issue certificates, marks and seals), that (inter alia):

- have the required expertise and are independent with regard to the subject matter of certification;
- have procedures to review and withdraw certifications, seals and marks;
- are able to deal with complaints about infringements of the certifications; and
- have rules to deal with conflicts of interest.

Criteria for accreditation will be developed by the supervisory authorities or the EDPB and will be publicly available.

Accreditations for certification bodies will be issued for a maximum of five years and are subject to renewals, as well as withdrawals in cases where conditions for the accreditation are no longer met.

The EDPB also published final guidelines on the accreditation of certification bodies. Note that the guidelines are primarily addressed to Member States, supervisory authorities and national accreditation bodies, and are not directly relevant to controllers and processors.

Where can I find this?

Codes of conduct
Articles 24, 28(5) 32, 40, 41, 57, 58, 64, 70, 83
Recitals 77, 81, 98, 99, 148, 168

Certifications, seals and marks
Articles 24, 25, 28, 32, 42, 43
Recitals 77, 81, 100, 166, & 168

Transfers of personal data

At a glance

- Transfers of personal data to recipients in "third countries" (i.e. outside the European Economic Area (*"EEA"*)) are restricted.
- The GDPR's obligations are broadly similar to those imposed by the Data Protection Directive, with some compliance mechanism improvements available, notably the removal of the need to notify standard contract clauses to supervisory authorities, and encouragement for the development of transfer adequacy codes of practice and certification schemes.
- Data transfer compliance remains a significant issue for multinational organisations and also for anyone using supply chains which process personal data outside the EEA.
- Breach of the GDPR's data transfer provisions is identified in the band of non-compliance issues for which the maximum level of fines can be imposed (up to 4% of worldwide annual turnover).
- Non-compliance proceedings can be brought against controllers and/or processors.

To do list

- ☑ Indentify all transfers of personal data; conduct transfer risk assessments and keep these under review; implement safeguards.
- ☑ Review questions included in standard procurement templates and contract clauses to ensure that information about your supplier's proposed transfer of personal data for which you are responsible is included.
- ☑ Review data transfers from the EEA to the UK; this will need to be mentioned in records of processing activity (and possibly privacy notices).
- ☑ If you transfer personal data outside the EEA whilst supplying goods or services, expect to be questioned by customers about your (and your supplier's) approach to compliance.

Commentary

Transfers of personal data to *"third countries"* (i.e. outside of the EEA) are restricted.

The Article 29 Working Party published guidelines on the interplay between the application of Article 3 GDPR and the provisions on international transfers as per Chapter V of the GDPR. This notes that GDPR does not define what a *"transfer"* is. The guidelines suggest three cumulative criteria: (i) the data exporter (a controller or processor) is subject to the GDPR for the given processing; (ii) the data exporter transmits or makes available the personal data to the data importer (a separate legal person which is a controller, joint controller or processor); and (iii) the data importer is in a third country or is an international organisation. One point underlined in the guidance is that controllers and processors which are subject to the GDPR on an extra-territorial basis (pursuant to Article 3(2)) will have to comply with Chapter V when they transfer personal data to a third country or to an international organisation.

The European Commission has the power to determine that certain countries, territories, specified sectors or international organisations offer an adequate level of protection for data transfers. The list of countries which have been approved by the European Commission is: Andorra, Argentina, Canada (where PIPEDA applies), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, Eastern Republic of Uruguay, New Zealand, the Republic of Korea, the United Kingdom, the United States of America (commercial organisations participating in the EU-US Data Privacy Framework). Countries to be added to or taken off this list shall be published in the Official Journal. Note however that data transferred from the EEA to the UK for the purposes of UK immigration control is not included in the adequacy decision.

The GDPR provides more detail on the particular procedures and criteria that the European Commission should consider when determining adequacy, stressing the need to ensure that the third country offers levels of protection that are *"essentially equivalent to that ensured within the Union"*, and providing data subjects with effective and enforceable rights and means of redress. The European Commission shall consult with the EDPB when assessing levels of protection and ensure that there is on-going monitoring and review of any adequacy decisions made (at least every four years). The European Commission also has the power to repeal, amend or suspend any adequacy decisions. The EDPB issued guidelines for the European Commission and the EDPB in November 2017 for the assessment of the adequacy of data protection in third countries.

Other methods of transferring personal data: Standard contractual clauses (SCCs) (either adopted by the Commission or adopted by a supervisory authority and approved by the European Commission) and binding corporate rules (BCRs) and legally binding and enforceable instruments between public authorities, are also accepted.

Significantly, transfers are also permitted where an approved code of conduct (based on the scheme in Article 40) or an approved certification mechanism (based on the scheme in Article 42) is used, provided that binding and enforceable commitments are made by the controller or processor in the third country to apply the appropriate safeguards, including as regards the data subjects' rights. There are also provisions for ad hoc safeguards to be agreed, subject to authorisation from the competent supervisory authority.

The EDPB issued guidance on codes of conduct as tools for transfers; as well as guidelines on accreditation of certification bodies under Article 43 of the GDPR.

Derogations (pursuant to Article 49 GDPR) permit transfers of personal data in limited circumstances, which include: explicit consent, contractual necessity, important reasons of public interest, legal claims, vital interests, and public register data. There is also a (limited) derogation for non-repetitive transfers involving a limited number of data subjects where the transfer is necessary for compelling legitimate interests of the controllers (which are not overridden by the interests or rights of the data subject) and where the controller has assessed (and documented) all the circumstances surrounding the data transfer and concluded there is adequacy. The controller must inform the supervisory authority and the data subjects when relying on this derogation. The EDPB issued guidelines on the derogations of Article 49 under the GDPR. It emphasied that this compelling legitimate interest derogation *"is envisaged by the law as a last resort".*

Finally, the GDPR makes it clear that it is not lawful to transfer personal data outside the EEA in response to a legal requirement from a third country, unless the requirement is based on an international agreement or one of the other grounds for transfer applies. The UK has opted out of this provision.

Further reading:

EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679

EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR

EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Schrems II)

Where can I find this?

Articles 44-50, Recitals 101-116

Appointment of supervisory authorities

At a glance

- Supervisory authorities are established in each Member State and are responsible for monitoring the application of the GDPR.
- They must co-operate with each other and with the European Commission, and contribute to the consistent application of the GDPR throughout the EU.
- They must act independently.
- Members of supervisory authorities must be appointed in a publicly transparent way and be skilled in data protection.
- There may be more than one supervisory authority in a country (e.g. where the country is composed of federal states).

To do list

- [ ] No action is required, but it is a good idea to establish or maintain a point of contact with your main supervisory authority.

Commentary

Supervisory authorities (also colloquially known as *"Data Protection Authorities"* or *"DPAs"*) are established in each Member State. They monitor the application of the GDPR to protect fundamental rights in relation to processing and to facilitate the free flow of personal data within the EU.

They have to co-operate with each other and the European Commission in order to contribute to the consistent application of the GDPR.

States such as Germany can (and do) have more than one supervisory authority, but one of them is nominated as the national representative in the EDPB.

Supervisory authorities must act with complete independence (subject to financial auditing and judicial supervision). The members of supervisory authorities remain free from external influence and must neither seek nor take instructions from anyone. Also, they must not act incompatibly with their duties nor, whilst in office, engage in an incompatible occupation, whether or not gainful.

Member States must provide their supervisory authorities with the human, technical, financial and other resources necessary to carry out all their tasks and exercise their powers effectively.

Each supervisory authority chooses its own staff and has sole direction of them. A supervisory authority's budget must be public and separately identified, even if part of the national budget.

Member State law must establish a supervisory authority, prescribe the rules for the authority's members, their qualifications and eligibility. The (renewable) term of office of a supervisory authority's members must be not less than four years. Members' duties of independence, outlined above, must be embodied in national law. Members of supervisory authorities and their staff are bound by a duty of *"professional secrecy"* both when in office and subsequently.

The provisions on setting up supervisory authorities are rather detailed - some points worth remarking on are: the specificity of the term of appointment, the emphasis on independence, the insistence on the provision of adequate resources for each supervisory authority, and the requirement that *"each member [of supervisory authorities] shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers."*

New EU data laws

The Data Act provides that where its provisions relate to processing of personal data, that data protection authorities will be competent for this processing and will be able to exercise the powers set out in the Data Act, as well as those under GDPR.

Where can I find this?

Recitals 117-123, Chapter VI Section 1, Articles 51-54

Competence, tasks and powers

At a glance

- Supervisory authorities are given specific competence to act on their own territory.
- The lead authority (where existent) has competence in cross-border cases (see section on co-operation and consistency between supervisory authorities for further details).
- Supervisory authorities are given an extensive list of specific powers and tasks.

To do list

- [ ] If you carry out cross-border processing, get to understand the lead-authority system (for which see section on co-operation and consistency between supervisory authorities). Identify which authority you think is your lead supervisory authority and prepare compliance measures accordingly, for instance, incident response plans (see 'Co-operation and consistency between supervisory authorities')
- [ ] Familiarise yourself with the comprehensive powers and tasks of supervisory authorities.

Competence

Each supervisory authority has competence *"for the performance of the tasks assigned to and the exercise of the powers conferred on it"* as described in the GDPR, on its national territory. Recital 122 tells us that this competence includes *"processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing in its territory"*.

In cases where the legal basis for processing, whether by a private body or a public authority, is compliance with a legal obligation, acting in the public interest or in the exercise of official authority, the supervisory authority of the relevant Member State has competence and the cross-border lead authority system is disapplied. The language is rather obscure, but Recital 128 says that a supervisory authority has exclusive jurisdiction over the processing that is carried out in the public interest both by public authorities and private bodies which in either case are established on the territory of the Member State of that supervisory authority. It is not clear whether this contemplates multiple establishments and is a means of excluding the one-stop shop or whether it gives exclusive jurisdiction to the home supervisory authority even if the processing is elsewhere in the EU. This might have wide application to private sector bodies – e.g. financial institutions carrying out anti-money-laundering activities in relation to customers elsewhere in the EU than their home country.

Supervisory authorities cannot exercise jurisdiction over courts acting in their judicial capacity. *'Court'* is not defined and it is not entirely clear how far down the judicial hierarchy this rule will extend.

A lead-authority system is set up to deal with cross-border processing (see section on co-operation and consistency between supervisory authorities for further information about this complex arrangement).

In the *Bundeskartellamt* case (C-252/21), the CJEU confirmed that a competition authority in a Member State could also reach a finding on whether an undertaking complied with data protection law, where this was relevant to a competition law query. The competition authority would have a duty of sincere co-operation with supervisory authorities for data protection.

Tasks

There is a very comprehensive list of tasks given to the supervisory authorities by Article 57 of the GDPR. There is no need to list them all, because the last on the list is *"fulfil any other tasks related to the protection of personal data"*. Supervisory authorities must therefore do anything that might reasonably be said to be about the *"protection of personal data"*.

Some tasks are worth emphasising. Supervisory authorities are to monitor and enforce the *"application"* of the GDPR and to promote awareness amongst the public, controllers and processors.

They are to advise their governments and parliaments on proposed new laws.

Helping data subjects, dealing with and investigating complaints lodged by individuals or representative bodies, conducting investigations and especially co-operating with other supervisory authorities are all specifically mentioned, as is monitoring the development of technical and commercial practices in information technology.

Supervisory authorities are to encourage the development of codes of conduct and certification systems and they are to *"draft and publish the criteria for accreditation"* of certification bodies and those which monitor codes of conduct.

Supervisory authorities cannot charge data subjects or Data Protection Officers for their services; the GDPR is however silent on whether controllers and processors could be charged fees in respect of services they receive from supervisory authorities.

Powers

Article 58 of the GDPR lists the powers of the supervisory authorities, to which Member States can add if they wish. Many of the powers correspond to the specific tasks listed in Article 57 and do not need repeating.

Worthy of mention are: ordering a controller or processor to provide information; conducting investigatory audits; obtaining access to premises and data; issuing warnings and reprimands and imposing fines; ordering controllers and processors to comply with the GDPR and data subjects' rights; banning processing and trans-border data flows outside the EU; approving standard contractual clauses and binding corporate rules. The exercise of powers by a supervisory authority must be subject to safeguards and open to judicial challenge.

Member States must give supervisory authorities the right to bring matters to judicial notice and *"where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation"*.

Finally, supervisory authorities must produce annual reports. In summary, the competence, powers and tasks of supervisory authorities are a comprehensive listing of everything a supervisory authority must or might do.

Where can I find this?

Recitals 117-123, WP 244, Chapter VI Section 2 Articles 55-59

Co-operation and consistency between supervisory authorities

At a glance

In cases of cross-border processing in the EU, supervisory authorities have to cooperate in order to ensure a consistent application of the GDPR. In qualifying cases, there is a lead authority, which will be the supervisory authority for the sole EU or main establishment ('one-stop-shop'). Supervisory authorities in other countries where a controller is established, or where data subjects are substantially affected, or authorities to whom a complaint has been made, can be involved in the cases, and the lead authority must co-operate with them.

To do list

- If you are a non-EU based controller or processor (and are caught by the long arm jurisdiction provisions of the GDPR), the lead authority system is irrelevant to you.

- If you just operate in one Member State, the supervisory authority for that Member State will be the lead authority for any cross-border processing. If you carry out activities in two or more Member States, find out if you meet the criteria to have a lead authority (taking into account the EDPB's guidance) and engage with that authority. Consider whether those responsible for data protection compliance in your organisation have suitable language skills to communicate with your lead authority.

Commentary

Lead Authority Competence

If a controller or processor carries out 'cross-border processing' either through multiple establishments in the EU or even through only a single establishment (where the processing is likely to substantially affect individuals in multiple Member States), the supervisory authority for the 'main' or single establishment acts as lead authority in respect of that cross-border processing.

The EDPB has adopted guidelines for identifying a lead supervisory authority. Where an organisation has multiple establishments, the main establishment and therefore the lead authority is determined by where the decisions regarding the purposes and manner of the personal data processing in question takes place - whilst this may be the place of central administration of the organisation, if decisions are actually taken in another establishment in the EU, the authority of that location is the lead authority. The guidelines recognise that there can be situations where more than one lead authority can be identified for different processing activities, i.e. in cases where a multinational company decides to have separate decision making centres, in different countries.

In relation to joint controllers, the guidelines have clarified that it is not possible to designate a common main establishment - and therefore, a lead authority - for both joint controllers. Each joint controller may have its own main establishment, but this cannot be considered the main establishment of the joint controllers for the processing that is carried out under their joint control.

Likewise, processors that provide services to multiple controllers do not really benefit from the one-stop-shop in cases involving their controllers, as the lead authority is the lead authority for each controller.

The guidelines also state that *"the GDPR does not permit 'forum shopping'"* – there must be an effective and real exercise of management activity or decision-making over the processing in the organisation's main establishment. Organisations should be able to demonstrate to supervisory authorities where decisions about data processing are actually taken and implemented, as they may be asked to evidence their position. The guidance notes that controllers without any establishment in the EU cannot benefit from the one-stop-shop mechanism (the mere presence of an EU representative does not trigger the one stop shop mechanism) – they must deal with local supervisory authorities in every Member State they are active in, through their local representative.

By derogation from the one-stop-shop, a national supervisory authority remains competent to exercise powers if a complaint is made to it or an infringement occurs on its territory and if the subject matter of the complaint or infringement relates only to an establishment on that territory or substantially affects data subjects only in that State. The EDPB guidelines contain guidance on the meaning of *'substantially affects'.*

Such 'local' cases have to be notified to the lead authority which has three weeks to decide whether or not to intervene (taking into account whether there is an establishment in the other state) in accordance with the co-operation procedure. If it does so, the non-lead authority can propose a decision to the lead authority.

If the lead authority does not intervene, the local authority handles the case using, where necessary, the mutual assistance and joint investigation powers.

In January 2019, the CNIL fined Google €50 million for GDPR breaches which had a cross border element. In light of Google's European operations being headquartered in Ireland (and the fact that Google considered the Irish DPC to be their lead authority), this decision was an interesting insight into how supervisory authorities are interpreting the cooperation and consistency mechanisms. In the CNIL's view, considering that the controller of the data processing at stake was Google LLC (and not Google France), Google Ireland Limited could not be considered as Google LLC's main establishment as it could not have any real and effective decision-making power over the relevant processing activities at the relevant point in time. Consequently, in the absence of a main establishment in the EU, Google LLC could not benefit from the lead authority mechanism and the CNIL believed it was competent to act pursuant to Articles 55 and 58. The CNIL's decision was upheld by the highest administrative court in France.

In June 2021, the CJEU ruled on a case referred to it by the Brussels Court of Appeal, concerning legal action brought by the Belgian DPA against Facebook for alleged GDPR infringements. The CJEU ruled that *under certain conditions*, a national supervisory authority may bring any alleged infringement of the GDPR before a court of its Member State, pursuant to Article 58(5) GDPR, even though that authority is not the lead supervisory authority. This is the case in principle when the non-lead authority is competent to adopt a decision finding that the processing infringes the GDPR under Article 56 and exercises this power with due regard to the GDPR's co-operation and consistency mechanism, whilst there is no pre-requisite that the controller has a main establishment or another establishment on the territory of that supervisory authority's Member State. The Court also confirmed the direct effect of Article 58(5) GDPR, which stipulates that EU Member States must provide that supervisory authorities have the power to bring GDPR infringements before judicial authorities and engage in legal proceedings where appropriate. This means that a supervisory authority can rely on this provision, even where this has not been specifically implemented in the legislation of the relevant Member State.

Where can I find this?

Recitals 124-138 and Chapter VII, Sections 1 & 2

Co-operation Procedure

The lead authority has to co-operate with other *"concerned"* supervisory authorities. They have to exchange information and try to reach consensus. A supervisory authority is *"concerned"* where the controller (or processor) has an establishment on the territory of that authority's Member State; where data subjects on that territory are (likely to be) substantially affected by the processing; or a complaint has been lodged with that authority.

The lead authority has to provide information to the other supervisory authorities concerned and it can seek mutual assistance from them and conduct joint investigations with them on their territories. The lead authority must submit a draft decision to concerned authorities without delay and they have four weeks in which to object. There can be another round of submitting draft decisions with a two-week objection period. If the lead authority does not wish to follow the views of concerned authorities, it must submit to the consistency procedure supervised by the EDPB.

There are detailed rules about which supervisory authority should adopt the formal decision and notify the controller, but the lead authority has the duty to ensure that, pursuant to a formal decision, compliance action is taken by a controller in all its establishments. A concerned supervisory authority can exceptionally, however, take urgent temporary action without waiting to complete the consistency process.

The lead authority system has a number of apparent weaknesses and could be undermined where non-lead authorities are able to assert themselves on the grounds that data subjects in their jurisdictions are substantially affected by processing conducted by a controller whose main establishment is elsewhere.

Mutual Assistance, Joint Operations & Consistency

Supervisory authorities are required to provide assistance to each other in particular in the form of information or carrying out *"prior authorisations and consultations, inspections and investigations"*. The European Commission can specify forms and procedures for mutual assistance.

Supervisory authorities can conduct joint investigations and enforcement operations. A supervisory authority has a right to be included in such operations if the controller or processor has an establishment on its territory or a significant number of its data subjects are likely to be substantially affected.

If local law permits, a host supervisory authority can give formal investigatory powers to seconded staff. Supervisory authorities have conducted joint investigations pre-GDPR, so the GDPR in practice has developed and strengthened these arrangements.

Where supervisory authorities take certain formal steps or disagree or wish for action to be taken by another supervisory authority, the GDPR provides for a consistency and dispute resolution mechanism.

The EDPB has to give opinions on various supervisory authority proposals, including the approval of binding corporate rules, certification criteria and codes of conduct. If a supervisory authority fails to request the opinion of the EDPB or does not follow an EDPB opinion, then the matter goes to the dispute resolution procedure.

The dispute resolution procedure also applies to lead authority/concerned authority disputes. In all these cases, the EDPB takes a binding decision on the basis of a two-thirds majority vote. If there is no such majority, then after a delay, a simple majority will suffice. The supervisory authorities involved are bound to comply and formal decisions have to be issued in compliance with the EDPB decision.

The most notable EDPB binding decisions under the co-operation and consistency mechanism concern the Irish DPA (the DPC) in cases regarding WhatsApp (July 2021 and December 2022) and the Facebook and Instagram services of Meta Platforms (July 2022 and December 2022). Following the EDPB's binding decision in the WhatsApp case of 2021, the DPC had to amend its draft decision regarding infringements of transparency, the calculation of the fine, and the period within which WhatsApp had to bring its processing into compliance. WhatsApp brought an action for annulment of the EDPB's binding decision before the CJEU, which was declared inadmissible (currently under appeal).

The far-reaching results of the consistency mechanism are also apparent in the EDPB's binding decisions of 2022 regarding the Instagram, Facebook and WhatsApp cases: in the first decision, concerning Instagram (July 2022), the EDPB instructed the DPC to amend its draft decision to include an infringement of Article 6(1) GDPR, after concluding that Instagram unlawfully processed children's personal data; also, to reassess the envisaged administrative

fine. In the decisions concerning Facebook and Instagram (December 2022), the EDPB instructed the DPC to include in its final decision an order for Meta to bring its processing of personal data for behavioural advertising into compliance with Article 6(1) GDPR within 3 months, and a finding of infringement of the fairness principle, as well as a requirement to adopt appropriate corrective measures. Also, the EDPB's binding decision led the DPC to significantly increase the fines in its final decisions (from a total of EUR 58 million in the draft decisions, to a total of EUR 390 million in the final decisions). The EDPB also decided that the DPC must carry out a new investigation regarding the processing of special categories of personal data. These decisions are currently being challenged in the CJEU.

A similar position was taken in the EDPB's binding decision of December 2022 in the WhatsApp case, whereby the EDPB instructed the DPC to include in its final decision an infringement of Article 6(1) GDPR and a corresponding administrative fine, and an infringement of the fairness principle, along with an order for WhatsApp to bring its processing operations into compliance within 3 months. The EDPB also decided that the DPC must carry out an additional investigation of WhatsApp's processing activities. This has created tension with the Irish DPA, which considered the EDPB's direction for further investigations problematic in jurisdictional terms and stated that it would take action for annulment before the CJEU, to the extent the direction may involve an overreach on the part of the EDPB.

Under Article 66, in exceptional circumstances where a supervisory authority considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the lead authority or consistency mechanism, immediately adopt provisional measures intended to produce legal decisions on its own territory which shall not exceed 3 months. This is what the Hamburg DPA relied upon when it opened administrative proceedings against Google (whose lead authority is the Irish DPC) in August 2019 in respect of Google's Speech Assistant system; it argued that effective protection of those affected *"from eavesdropping, documenting and evaluating private conversations by third parties can only be achieved by prompt execution".*

Where a supervisory authority has taken provisional measures under the urgency procedure and considers that *final* measures need urgently to be adopted, it may request an urgent opinion or urgent binding decision from the EDPB. The first such urgent binding decision was adopted by the EDPB in July 2021, following a request from the Hamburg DPA, which had ordered as a provisional measure the ban on processing of WhatsApp user data by Facebook for the latter's own purposes. The EDPB concluded that the conditions to demonstrate the existence of an infringement and an urgency were not met and decided that no final measures needed to be adopted by the lead supervisory authority (the Irish DPA).

The EDPB has also looked at the cooperation and consistency mechanisms in some detail as part of its contribution to the evaluation of GDPR under Article 97 (adopted on 18 February 2020) and has issued guidelines on this topic. It highlights that the implementation of the lead authority mechanism remains challenging and its success going forward will depend on the consistent interpretation of key GDPR terms, the alignment of national administrative procedures, adequate human and financial resources of supervisory authorities, further improvement of communication tools and reasonable timeframes for case handling.

Where can I find this?

Recitals 124-138 and Chapter VII, Sections 1 & 2

European Data Protection Board

At a glance

- The Article 29 Working Party, whose members were the EU's national supervisory authorities, the European Data Protection Supervisor (*"EDPS"*) and the European Commission, was transformed into the European Data Protection Board (*"EDPB"*), with similar membership but an independent Secretariat.
- The EDPB has the status of an EU body with legal personality and extensive powers to determine disputes between national supervisory authorities, to give advice and guidance and to approve EU-wide codes and certification.

To do list

No action is required.

Commentary

As of 25 May 2018, the EDPB replaced the Article 29 Working Party, which was established under the Data Protection Directive. The EDPB is an EU body which consists of the heads of national supervisory authorities (or their representatives) and the EDPS.

The European Commission representative on the EDPB is a non-voting member and in states (such as Germany) with multiple supervisory authorities, the national law must arrange for a joint representative to be appointed. In dispute resolution cases, where a binding decision is to be given, the EDPS voting powers are restricted to circumstances in which the principles of the case would be applicable to the EU institutions.

The EDPB has a much enhanced status. It is not merely an advisory committee, but an independent body of the European Union with its own legal personality.

It is formally represented by its Chair, who has the chief role in organising the work of the EDPB and particularly in administering the conciliation procedure for disputes between national supervisory authorities. The Chair and two Deputies are elected from the membership of the EDPB and serve for five years, renewable once.

The EDPB normally decides matters by a simple majority, but rules of procedure and binding decisions (in the first instance) are to be determined by a two-thirds majority.

The EDPB has adopted its own rules of procedure and organizational rules. The independence of the EDPB is emphasised. There seems to be an implicit suggestion that the Commission had exercised too great an influence over the Article 29 Working Party in the past and was seeking to consolidate this power.

The EDPB has its own Secretariat provided by the EDPS, but which acts solely under the direction of the Chair of the EDPB.

The EDPB is provided with a long and detailed list of tasks, but its primary role is to contribute to the consistent application of the GDPR throughout the Union. It advises the European Commission, in particular on the level of protection offered by third countries or international organisations, and promotes cooperation between national supervisory authorities. It issues guidelines, recommendations and statements of best practice: for example, on matters such as when a data breach is *"likely to result in a high risk to the rights and freedoms"* of individuals or on the requirements for Binding Corporate Rules. Note that during its first plenary meeting, the EDPB endorsed the GDPR related Article 29 Working Party Guidelines which had been published to date.

The EDPB's most distinctive role is to conciliate and determine disputes between national supervisory authorities. For more about that activity, see the section on competence, tasks and powers. The old Article 29 Working Party was often criticised for not consulting adequately before taking decisions. The EDPB is required to consult interested parties *"where appropriate"*. Notwithstanding the *"get-out"* qualification, this is a major benefit to those who may be affected by opinions, guidelines, advice and proposed best practice.

EDPB discussions are to be *"confidential where the Board deems it necessary, as provided for in its rules of procedure"*. This suggests that meetings and discussions will, in principle, be public unless otherwise determined.

Finally, the EDPB publishes Annual Reports.

Further reading:

EDPB Guidelines and reports:

EDPB Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679

EDPB Guidelines 02/2022 on the application of Article 60 GDPR

EDPB Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority

Contribution of the EDPB to the evaluation of the GDPR under Article 97

EDPB binding decisions:

Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR

Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR

Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Article 65 GDPR)

Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Article 65 GDPR)

Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Article 65 GDPR)

Urgent Binding Decision 01/2021 on the request under Article 66(2) GDPR from the Hamburg (German) Supervisory Authority for ordering the adoption of final measures regarding Facebook Ireland Limited

Court cases

Case C-645/19, *Facebook Ireland Ltd, Facebook Inc., Facebook Belgium BVBA, v Gegevensbeschermingsautoriteit*

Case T-709/21, *WhatsApp Ireland v European Data Protection Board*

T-129/23, *Meta Platforms Ireland v European Data Protection Board*

Case C252/21, *Meta Platforms Inc., Meta Platforms Ireland Limited, Facebook Deutschland GmbH v Bundeskartellamt*

CNIL v Google, Decision of 21 January 2019 (EDPB summary) and French Supreme Court decision upholding CNIL's decision (in French only)

Where can I find this?

Recitals 139 & 140, and Chapter VII Section 3

Remedies and liabilities

At a glance

- Individuals have the following rights (against controllers and processors):
  - the right to lodge a complaint with supervisory authorities where their personal data has been processed in a way that does not comply with the GDPR;
  - the right to an effective judicial remedy where a competent supervisory authority fails to deal properly with a complaint;
  - the right to an effective judicial remedy against a relevant controller or processor; and
  - the right to compensation from a relevant controller or processor for material or non-material damage resulting from infringement of the GDPR.
- Both natural and legal persons have the right of appeal to national courts against a legally binding decision concerning them made by a supervisory authority.
- Individuals can bring claims for non-pecuniary loss. The potential for actions to be brought by representative bodies is facilitated.
- Judicial remedies and liability for compensation extend to both data controllers and data processors who infringe the Regulation.

To do list

- [ ] Controllers and their processors should ensure that data processing agreements and contract management arrangements clearly specify the scope of the processor's responsibilities and should agree to mechanisms for resolving disputes regarding respective liabilities to settle compensation claims.
- [ ] Controllers and processors should agree to report to other controllers or processors that are involved in the same processing, any relevant compliance breaches and any complaints or claims received from relevant data subjects.

Complaints to supervisory authorities

The rights of data subjects to complain to supervisory authorities are slightly strengthened as compared to the Data Protection Directive. The Directive obliged supervisory authorities to hear claims lodged by data subjects to check the lawfulness of data processing and inform data subjects that a check had taken place.

Under the GDPR, data subjects whose personal data are processed in a way that does not comply with the GDPR have a specific right to lodge a complaint with supervisory authorities and supervisory authorities must inform data subjects of the progress and outcome of the complaints.

Judicial remedies against decisions of supervisory authorities

Both data subjects and other affected parties have rights to an effective judicial remedy in relation to certain acts and decisions of supervisory authorities.

- Any person has the right to an effective judicial remedy against legally binding decisions concerning him/her, taken by a supervisory authority.
- Data subjects have the right to an effective judicial remedy where a supervisory authority fails to deal with a complaint or fails to inform the data subject within 3 months of the progress or outcome of his or her complaint.

Recital 143 of the GDPR explains that decisions and actions that may be challenged in the courts include the exercise of investigative, corrective, and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. The right does not encompass other measures by supervisory authorities which are not legally binding, such as opinions issued or advice provided by supervisory authorities.

Judicial remedies against data controllers & data processors

Data subjects whose rights have been infringed have the right to an effective judicial remedy against the data controller or processor responsible for the alleged breach. This extends beyond the equivalent provision previously contained in the Data Protection Directive, which provided a judicial remedy only against data controllers but not against data processors.

Liability for compensation

Any person who has suffered damage as a result of infringement of the GDPR has the right to receive compensation from the controller or the processor. Previously, under the Data Protection Directive, liability for compensation was limited to controllers only.

The following provision is made for the allocation of liability for compensation between controllers and processors:

- controllers are liable for damage caused by processing which is not in compliance with the GDPR;

- processors are liable only for damage caused by any processing in breach of obligations specifically imposed on processors by the GDPR, or caused by processing that is outside, or contrary to lawful instructions of the controller; and

- in order to ensure effective compensation for data subjects, controllers and processors that are involved in the same processing and are responsible for any damage caused, each shall be held liable for the entire damage. However, a processor or controller that is held liable to pay compensation on this basis is entitled to recover from other relevant parties, that part of the compensation corresponding to their part of the responsibility for the damage.

Whilst the Data Protection Directive referred only to the right to compensation for *"damage"*, the GDPR makes clear that compensation may be recovered for both pecuniary and non-pecuniary losses. This clarification is, however, consistent with current English law interpretation of the meaning of damage for the purpose of compensation claims previously made under the Data Protection Act 1998 (see *Google Inc. v Vidal-Hall & Others* [2015] EWCA Civ 311).

The CJEU in the *Österreichische Post* case (case C-300/21) determined that the right to compensation provided for by the GDPR is subject to three cumulative conditions: (i) infringement of the GDPR, (ii) material or nonmaterial damage resulting from that infringement and (iii) a causal link between the damage and the infringement. As such, a mere infringement of the GDPR does not give rise to a right to compensation. The CJEU also held that there is no requirement for the non-material damage suffered to reach a certain threshold of seriousness in order to confer a right to compensation.

In December 2023 the CJEU further explored these issues in the case C-340/21 – *Natsionalna agentsia za prihodite*, involving the Bulgarian National Revenue Agency (the NAP). The Court determined that the fear of a possible misuse of personal data is capable, in itself, of constituting non-material damage. However, where a person claiming compensation on that basis relies on the fear that his or her personal data will be misused in the future owing to the existence of such an infringement, the national court dealing with the case must verify that that fear can be regarded as well founded, in the specific circumstances at issue and with regard to the data subject.

The GDPR provides that controllers and processors are exempt from liability if they are *"not in any way responsible for the event giving rise to the damage"*. This exemption appears to be slightly narrower than the exemption that could be claimed under the Data Protection Directive by a controller who could prove *"that he is not responsible for the event giving rise to the damage"*.

Representative bodies

The GDPR entitles representative bodies, acting on behalf of data subjects, to lodge complaints with supervisory authorities and seek judicial remedies against a decision of a supervisory authority or against data controllers or processors. The provision applies to any representative body that is:

- a not-for-profit body, organisation or association;
- properly constituted according to Member State law;
- with statutory objectives that are in the public interest; and
- active in the field of data protection.

Data subjects may also mandate such bodies to exercise on their behalf rights to recover compensation from controllers or processors provided this is permitted by Member State law.

Where empowered to do so by Member State law, such representative bodies may, independently of a data subject's mandate, lodge complaints with supervisory authorities and seek judicial remedies against decisions of a supervisory authority or against data controllers or processors.

The CJEU in *Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.* (C-319/20) confirmed that Article 80(2) of the GDPR must be interpreted as not precluding national legislation which allows a consumer protection association to bring legal proceedings for infringements of laws protecting personal data in the absence of a mandate conferred on it for that purpose and independently of the infringement of specific rights of the data subjects.

There were no equivalent provisions in the Data Protection Directive.

Where can I find this?

Articles 77-82, Recitals 141-147

Administrative fines

At a glance

- Supervisory authorities are empowered to impose significant administrative fines on both data controllers and data processors.
- Fines may be imposed instead of, or in addition to, measures that may be ordered by supervisory authorities. They may be imposed for a wide range of contraventions, including purely procedural infringements.
- Administrative fines are discretionary rather than mandatory; they must be imposed on a case by case basis and must be *"effective, proportionate and dissuasive"*.
- There are two tiers of administrative fines:
  - Some contraventions will be subject to administrative fines of up to €10,000,000 or, in the case of undertakings, 2% of global turnover, whichever is higher.
  - Others will be subject to administrative fines of up to €20,000,000 or, in the case of undertakings, 4% of global turnover, whichever is higher.
- Member States may determine whether, and to what extent public authorities should be subject to administrative fines.

General considerations

Administrative fines are not applicable automatically and are to be imposed on a case by case basis. Recital 148 clarifies that in the case of a minor infringement, or where a fine would impose a disproportionate burden on a natural person, a reprimand may be issued instead of a fine. In its guidelines on the application and setting of administrative fines, the EDPB says supervisory authorities must assess all the facts of the case in a manner that is consistent and objectively justified. In particular, supervisory authorities must assess what is effective, proportionate and dissuasive in each case to meet the objective pursued by the corrective measure chosen, i.e. to re-establish compliance with rules, or to punish unlawful behaviour (or both).

There used to be a high degree of variation across Member States in relation to the imposition of financial penalties by supervisory authorities. Although arrangements under the GDPR make provision for maximum penalties and allow supervisory authorities a degree of discretion in relation to their imposition, Recital 150 indicates that the consistency mechanism may be used to promote a consistent application of administrative fines. This is reinforced in the EDPB's guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (3 October 2017) (WP253), which push for a harmonised approach by means of active participation and information exchange among supervisory authorities to ensure that equivalent sanctions are imposed for similar cases.

On the 12 May 2022, the EDPB released its draft guidelines on the calculation of fines under the GDPR which were subsequently finalised and adopted in June 2023. The aim of the guidelines is to harmonise the methodology supervisory authorities use when calculating the amount of the fine and complement the aforementioned EDPB guidelines on the application and setting of administrative fines. The guidelines set out a 5-step calculation methodology: (i) DPAs have to establish whether the case at stake concerns one or more instances of sanctionable conduct and if they have led to one or multiple infringements (to clarify if all the infringements or only some of them can be fined); (ii) DPAs have to rely on a starting point for the calculation of the fine for which the EDPB provides a harmonised method; (iii) DPAs have to consider aggravating or mitigating factors that can increase or decrease the amount of the fine, for which the EDPB provides a consistent interpretation; (iv) DPAs must determine the legal maximums of fines as set out in Article 83 (4)-(6) GDPR and ensure that these amounts are not exceeded; and (v) DPAs need to analyse whether the calculated final amount meets the requirements of effectiveness, dissuasiveness and proportionality or whether further adjustments to the amount are necessary.

Maximum administrative fines

The GDPR sets out two sets of maximum thresholds for administrative fines that may be imposed for relevant infringements.

In each case, the maximum fine is expressed in € (euro) or, in the case of undertakings, as a percentage of total worldwide annual turnover of the preceding year, whichever is higher. Recital 150 confirms that in this context *"an undertaking"* should be understood as defined in Articles 101 and 102 of the Treaty on the Functioning of the European Union *("TFEU")* (i.e. broadly speaking, as entities engaged in economic activity).

Infringement of the following GDPR provisions is subject to administrative fines up to €20,000,000 or in the case of undertakings, up to 4% of global turnover, whichever is higher:

- the basic principles for processing, including conditions for consent (Articles 5, 6, 7 and 9);
- data subjects' rights (Articles 12-22);
- international transfers (Articles 44-49);
- obligations under Member State laws adopted under Chapter IX; and

- non-compliance with an order imposed by supervisory authorities (as referred to in Article 58(2)) or a failure to comply with a supervisory authority's investigation under Article 58(1).

Other infringements are subject to administrative fines up to €10,000,000 or, in the case of undertakings, up to 2% of global turnover, whichever is higher. Contraventions subject to these maximum fines include infringement of the following obligations:

- to obtain consent to the processing of data relating to children (Article 8);
- to implement technical and organisational measures to ensure data protection by design and default (Article 25);
- on joint controllers to agree to their respective compliance obligations (Article 26);
- on controllers and processors not established in the EU to designate representatives (Article 27);
- on controllers in relation to the engagement of processors (Article 28);
- on processors to subcontract only with the prior consent of the controller and to process data only on the controller's instruction (Articles 28-29);
- to maintain written records (Article 30);
- on controllers and processors to co-operate with supervisory authorities (Article 31);
- to implement technical and organisational measures (Article 32);
- to report breaches when required by the GDPR to do so (Articles 33-34);
- in relation to the conduct of privacy impact assessment (Articles 35-36);
- in relation to the appointment of Data Protection Officers (Articles 37-39);
- imposed on certification bodies (Article 42-43); and
- imposed on monitoring bodies to take action for infringement of codes of conduct (Article 41).

In cases where the same or linked processing involves violation of several provisions of the GDPR, fines may not exceed the amount specified for the most serious infringement.

In December 2023 the CJEU delivered judgment in Case C-683/21, involving the National Public Health Centre under the Lithuanian Ministry of Health. It found as a matter of general principle that a controller can be found liable and be fined for the actions of a processor, performing data processing operations on behalf of that controller, unless the processor was acting in a way that was incompatible with the arrangements previously agreed with the controller.

Factors to be taken into account

Article 83(2) lists factors to be taken into account by a supervisory authority when determining whether to impose an administrative fine and deciding on the amount of any fine to be imposed. These include:

- the nature, gravity and duration of the infringement having regard to the nature, scope or purpose of the processing concerned as well as the number of data subjects and level of damage suffered by them;
- whether the infringement is intentional or negligent;
- actions taken by the controller or processor to mitigate the damage suffered by data subjects;
- the degree of responsibility of the controller or processor;
- any relevant previous infringements;
- the degree of co-operation with the supervisory authority;
- categories of personal data affected;
- whether the infringement was notified by the controller or processor to the supervisory authority;
- any previous history of enforcement;

- adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

- any other aggravating or mitigating factors applicable to the circumstances of the case (e.g. financial benefits gained, losses avoided, directly or indirectly, from the infringement).

Where fines are imposed on persons that are not an undertaking, the supervisory authority should also take account of a person's economic situation.

In setting the level of administrative fines within each threshold, the EDPB's guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 require that supervisory authorities assess all the facts of the case in a manner that is consistent and objectively justified.

Derogations and special conditions

At a glance

Under the GDPR Member States retain the ability to introduce derogations where these are required for the purposes of national security, prevention and detection of crime and in certain other situations. In line with case law of the Court of Justice of the European Union, any such derogation must respect *"the essence"* of the right to data protection and be a necessary and proportionate measure.

The GDPR either requires or permits Member States to introduce supplemental laws for certain special purposes. In the case of historical and scientific research, statistical processing and archiving, this can even provide a lawful basis for processing special categories of data.

Other special topics where Member State law is foreseen by the GDPR include processing of employee data, processing in connection with freedom of expression and professional secrecy (where restrictions of supervisory authority audit rights are foreseen).

Controllers (and, in some cases, processors) need to check for and adjust to different Member State approaches in these areas.

Local variations should be considered as they are significant in many areas, e.g. HR data processing.

To do list

- [ ] Assess whether any processing you carry out may be subject to derogations or special conditions under the GDPR, and check what has been implemented in Member State laws applicable to you.

Commentary

Special cases

The GDPR contains broad derogations and exemptions in two main areas: (1) in Chapter III Section 5, regarding *"restrictions"* to obligations and data protection rights; and (2) in Chapter IX, regarding *"specific processing situations"*. The EU Commission's Directorate-General for Justice and Consumers published a report, summarising Member States' implementation of these specific provisions in January 2021.

Article 23 – Restrictions

Article 23 of the GDPR created the right for Member States to introduce derogations in certain situations. Member States are able to introduce derogations from transparency obligations and data subject rights, but only where the measure *"respects the essence of … fundamental rights and freedoms and is … necessary and proportionate … in a democratic society"*.

Any derogation must safeguard one of the following:

- national security;
- defence;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences or breaches of ethics in regulated professions;
- other important public interests, in particular economic or financial interests (e.g. budgetary and taxation matters);
- the protection of judicial independence and proceedings;
- the exercise of official authority in monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
- the protection of the data subject, or the rights and freedoms of others; or
- the enforcement of civil law matters.

In order for a measure to be acceptable, it must (in accordance with Article 23(2)) include specific provisions setting out:

- the purposes of processing;
- the affected categories of data;
- the scope of the restrictions to the GDPR which are introduced by the measure;
- safeguards to prevent abuse, unlawful access or transfer;
- the controllers who may rely on the restrictions;
- the applicable retention periods and security measures;
- the risk to data subjects' rights and freedoms; and
- the right of data subjects to be informed about the restriction, unless this is prejudicial to the purpose of the restriction.

Articles 85-91: "Specific Data Processing Situations"

The provisions in Chapter IX GDPR provide for a mixed set of derogations, exemptions and powers to impose additional requirements, in respect of GDPR obligations and rights, for particular types of processing.

Article 85: Freedom of expression and information

This provision requires Member States to introduce exemptions to the GDPR where necessary to *"reconcile the right to the protection of personal data with the right to freedom of expression and information."* Article 85(2) makes specific provision for processing carried out for journalistic purposes, or for the purposes of academic, artistic or literary expression. Member States were required to notify the European Commission on how they implemented this requirement and of any changes to such laws.

Article 86: Public access to official documents

This provision allows personal data within official documents to be disclosed in accordance with Union or Member State laws which allow public access to official documents. This is not without limit - such laws should, according to Recital 154 GDPR, *"reconcile public access to official documents...with the right to protection of personal data"*.

Article 87: National identification numbers

This maintains the right of Member States to set their own conditions for processing national identification numbers, provided appropriate safeguards are in place.

Article 88: Employee data

Member States are permitted to establish (either by law or through collective agreements) more specific rules in respect of the processing of employee personal data, covering every major aspect of the employment cycle from recruitment to termination. This includes the ability to implement rules setting out when consent may be deemed valid in an employment relationship. Such rules must include specific measures to safeguard the data subject's *"dignity, legitimate interests and fundamental rights"* and the GDPR cites transparency of processing, intragroup transfers and monitoring systems as areas where specific regard for these issues is required. Member States must notify the European Commission of any laws introduced under this Article, and must also notify it of any amendments. Details on this can be found on the European Commission website.

Article 89(1) and (2): Scientific and historical research purposes or statistical purposes

Article 89(1) acknowledges that controllers may process data for these purposes where appropriate safeguards are in place (see sections on lawfulness of processing and further processing and Special categories of data and lawful processing). Where possible, controllers are required to fulfil these purposes with data which does not permit, or no longer permits, the identification of data subjects; if anonymisation is not possible, pseudonymisation should be used, unless this would also prejudice the purpose of the research or statistical process. Useful comments on pseudonymisation were published by ENISA in their January 2019 report entitled *"Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation"*, and guidelines on anonymization feature in the EDPB's work programme for 2023-2024.

Article 89(2) allows Member States and the EU to further legislate to provide derogations from data subject rights to access, rectification, erasure, restriction and objection (subject to safeguards as set out in Article 89(1)) where such rights *"render impossible or seriously impair"* the achievement of these specific purposes, and derogation is necessary to meet those requirements.

The recitals add further detail on how *"scientific research"*, *"historical research"* and *"statistical purposes"* should be interpreted. Recital 159 states that scientific research should be *"interpreted in a broad manner"* and includes privately funded research, as well as studies carried out in the public interest. In order for processing to be considered statistical in nature, Recital 162 says that the result of processing should not be *"personal data, but aggregate data"* and should not be used to support measures or decisions regarding a particular individual.

Article 89(1) and (3): Archiving in the public interest

The same derogations and safeguards exist for *"archiving in the public interest"* as are mentioned above in respect of processing for research and statistical purposes, except that derogations may also be granted for the right to data portability. Further detail is included in Recital 158, which suggests that this should only be relied upon by bodies or authorities that have an obligation to interact with records of *"enduring value for general public interest"* under Member State or Union law.

Article 90: Obligations of secrecy

This Article allows Member States to introduce specific rules to safeguard *"professional"* or *"equivalent secrecy obligations"* where supervisory authorities are empowered to have access to personal data or premises. These rules must *"reconcile the right to protection of personal data against the obligations of secrecy"*, and can only apply to data received or obtained under such obligation. Again, Member States must notify the European Commission of any laws introduced under this Article and must also notify it of any amendments. Details on this can be found on the European Commission website.

Article 91: Churches and religious associations

This Article protects *"comprehensive"* existing rules for churches, religious associations and communities where these are brought into line with the GDPR's provisions. Such entities will still be required to submit to the control of an independent supervisory authority under the conditions of Chapter VI (see section on co-operation and consistency between supervisory authorities).

Where can I find this?

Derogations
Article 23, Recital 73
Special conditions
Articles 6(2), 6(3), 9(2)(a), 85-91
Recitals 50, 53, 153-165

Delegated acts, implementing acts and final provisions

At a glance

As prescribed by the final chapters of the GDPR, the GDPR took effect on 25 May 2018. The GDPR's intended relationship with other EU data protection instruments including Directive 2002/58/EC (the *"e-Privacy Directive"*) is also set out in these chapters.

The European Commission will report regularly on the GDPR. These final provisions also empower the European Commission to adopt certain delegated acts under the GDPR (e.g. in respect of the use of icons and certification mechanisms).

Commentary

Chapter 10 of the GDPR grants the European Commission the power to adopt delegated acts (as referred to in Article 12(8) in respect of standardised icons and in Article 43(8) in respect of certification mechanisms). These delegated legislative powers can be revoked by the Parliament or the Council at any time. Delegated acts enter into force no earlier than 3 months after being issued, and only if neither the Parliament nor the Council objects. The European Commission will be assisted by a committee, in accordance with Regulation 182/2011. It is of particular importance that the European Commission carry out appropriate consultations when carrying out its preparatory work, including at expert level (Recital 166).

Implementing powers are also conferred on the European Commission in order to ensure uniform conditions for the implementation of the GDPR which should also be exercised in accordance with Regulation 182/2011.

Chapter 11 of the GDPR confirms that the Data Protection Directive was repealed on 25 May 2018. References in other legislation to the repealed Data Protection Directive are now construed as references to the GDPR, and references to the Article 29 Working Party are now construed as references to the EDPB.

The European Commission will report regularly on the GDPR to the Parliament and the Council, with particular focus on the GDPR's data transfer, co-operation and consistency provisions. The first report was published on 24 June 2020, and new reports will follow every 4 years thereafter, with the next being due in June 2024. The reports will be made public.

Article 95 makes clear that the GDPR must be interpreted so as to not impose additional obligations on providers of publicly available electronic communications services in the Union to the extent that they are subject to specific obligations under the e-Privacy Directive (2002/58/EC, as amended) that have the same objectives. A new EU Privacy Regulation was proposed by the European Commission, in early 2017, to replace the e-Privacy Directive; however, the European Parliament and Council have so far failed to reach agreement on the final text.

Recital 171 clarifies that where processing is based on a consent obtained before the GDPR came into force, it is not necessary for the individual to give their consent again if the way the consent was given is in line with the conditions of the GDPR.

Where can I find this?

Articles 92-99, Recitals 166-173

About Us
A leading data protection and technology-focussed law firm

Data protection experts

We are top ranked in legal directories and we boast one of the largest practices in Europe and Asia Pacific. We have a deep understanding of changes in technology and law. Our clients often collect large quantities of sensitive data and are high profile businesses, for whom the disclosure or misuse of data will have severe ramifications.

A number of our lawyers are former members of data protection authorities. Some of our lawyers have also spent time in-house, giving the team hands-on experience, and reinforcing a pragmatic, collaborative approach to providing legal services for our clients.

Global coverage

We have 1,400 lawyers worldwide across a global network spanning 32 offices in 23 countries.

- ***Bird & Bird office locations:*** Abu Dhabi • Amsterdam • Beijing • Bratislava • Brussels • Budapest • Casablanca • Copenhagen • Dubai • Dublin • Dusseldorf • Frankfurt • The Hague • Hamburg • Helsinki • Hong Kong • London • Luxembourg • Lyon • Madrid • Milan • Munich • Paris • Prague • Rome • San Francisco • Shanghai • Singapore • Stockholm • Sydney • Warsaw • Shehzen

- ***Bird & Bird Plus Firms:*** Building a collaborative network so that we can offer clients a joined-up, international legal service with affiliated law firms

Contact us

Reach out to one of our team if you have a data protection query.

twobirds.com

Bird & Bird